Managed 24-port 10/100Base-TX
plus 4-slot Gigabit Combo (RJ45/SFP)
Layer 3 Access Switch

NSH-580

V 1.0.5

User Manual

(February 2008)

VOLKTEK
Optical Ethernet Experts

COPYRIGHT

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photo copying, recording or otherwise, without the prior written permission of the publisher.

FCC WARNING

This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at the user's own expense.

CE

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

CAUTION

RISK OF EXPLOSION IF A BTTERY IS REPLACED BY AN INCORRECT TYPE, DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

Take special care to read and understand all the content in the warning boxes:

Warning

TABLE OF CONTENTS

1 ABOUT THIS GUIDE....5

1.1 Welcome....5
1.2 Purpose....5
1.3 Terms/Usage....5
1.4 Features....5
1.5 Specifications....6

2 HARDWARE DESCRIPTION....9

2.1 Product Illustration....9
2.2 Connectors....10
2.2.1 10/100Base-TX Ports....10
2.2.2 10/100/1000Base-T Ports....10
2.2.3 SFP slots for SFP modules....10

3 INSTALLATION....11

3.1 Desktop installation....11
3.2 Mounting on a rack....11
3.3 Getting Connected....11
3.4 Powering On the Unit....12
3.5 Installing the SFP modules and Fiber Cable....12
3.6 Connecting Copper Cable....14
3.7 Connecting the Console Port Cable....14
3.8 Connecting to computers or a LAN....14
3.9 Power On the Unit....14

4 LED INDICATORS....15

5 MANAGEMENT OPTIONS....16

5.1 Web-based Management Interface....16
5.2 SNMP-Based Management....16
5.3 Configuring the Switch via Console Port (RS-232 DCE)....16
5.3.1 Using HyperTerminal to Set IP address....16
5.4 Telnet and SSH....18
5.5 SNMP Settings....20
5.6 Traps....20
5.7 MIBs....20

6 FIRST TIME CONNECTING TO THE SWITCH....21

7 WEB MANAGEMENT 24

7.1 Log into Web Management 24
7.1.1 Standard GUI buttons 25
7.2 System 25
7.2.1 Management 25
7.2.2 IP Setup 26
7.2.3 Reboot 27
7.2.4 Firmware Upgrade 27
7.3 Physical Interface 28
7.3.1 Port Status 28
7.4 IP Interface 29
7.5 Router Reports 30
7.6 Routing 31
7.6.1 Static Route 31
7.6.2 RIP 32
7.6.3 OSPF 34
7.6.4 Multicast Route 37
7.6.5 VRRP 40
7.7 Bridge 41
7.7.1 Spanning Tree 41
7.7.2 Link Aggregation Static 46
7.7.3 LACP 47
7.7.4 Mirroring 51
7.7.5 Static Multicast 52
7.7.6 IGMP Snooping 53
7.7.7 Traffic Control 55
7.7.8 Dynamic Addresses 55
7.7.9 Static Addresses 56
7.7.10 VLAN Configuration 57
7.7.11 GVRP 58
7.7.12 QoS/CoS 60
7.8 SNMP 62
7.8.1 Host Table 62
7.8.2 Trap Setting 63
7.8.3 SNMPv3 VGU Table 64
7.9 ACL 66
7.9.1 Set Access Control List 66
7.9.2 Apply Access Control List 68
7.9.3 Content Aware 69
7.10 Security 70
7.10.1 Port Access Control 70
7.10.2 Dial-in User 72
7.10.3 RADIUS 72
7.10.4 IP DHCP Snooping 73
7.11 Traffic Chart 75
7.11.1 Traffic Comparison Chart 75
7.11.2 Group Chart 76
7.11.3 History Chart 77
7.12 Save Configuration 77

8 COMMAND LINE INTERFACE 78

8.1 Power On 78
8.1.1 Boot ROM command mode 78
8.1.2 Boot ROM Commands 78

8.2 Login and Logout 79
8.3 CLI Commands 79
8.3.1 User Account 79
8.3.2 Backup and Restore 80
8.3.3 System Management Configuration 80
8.3.4 Physical interface commands 83
8.3.5 IP interface 84
8.3.6 RIP 86
8.3.7 OSPF 86
8.3.8 VRRP 87
8.3.9 Spanning Tree 87
8.3.10 Link Aggregation 88
8.3.11 LACP 88
8.3.12 Mirroring 89
8.3.13 Static Multicast 90
8.3.14 IGMP Snooping 91
8.3.15 Traffic Control 91
8.3.16 Dynamic Addresses 92
8.3.17 Static Addresses 93
8.3.18 VLAN 93
8.3.19 GVRP 94
8.3.20 CoS/QoS 95
8.3.21 SNMP 96
8.3.22 Filter 96
8.3.23 Port Access Control 97
8.3.24 Dial-in User 99
8.3.25 RADIUS 99
8.4 Miscellaneous commands 99

9 CONTACT INFORMATION 100

1 About This Guide

1.1 Welcome

Congratulations on choosing the NSH-580 Managed 24-port 10/100Base-TX + 4-port Gigabit Combo Layer 3 Access Switch. The NSH-580 is a high-performance managed SNMP Layer 3 switch that provides users with twenty four 10/100Mbps Ethernet and 4 Gigabit Combo ports with both SFP slot and RJ-45. The Web/SNMP management provides remote control capability that provides flexible network management and monitoring options. Whether managed via an "in-band" SNMP management station, an internet web browser, or via an "out-of-band" RS-232 console port, the NSH-580 facilitates network operational control and diagnostics.

For increased bandwidth applications, the NSH-580 can accommodate trunk groups with a maximum of 8 ports in each trunk.

Moreover, these trunk ports are with fair-over function to provide redundant backup if one or more of the ports are malfunctioning. It also supports both port-based VLAN and tag-based VLAN, thereby simplifying network traffic segmentation, broadcast domain extension and other associated benefits of VLANs.

This abundance of features together with Layer 3 routing functions translate into increased efficiency and performance in network administration.

1.2 Purpose

This guide discusses how to install and configure your Managed Layer 3 Access Switch.

1.3 Terms/Usage

In this guide, the term “Switch” (first letter upper case) refers to the NSH-580 Switch, and “switch” (first letter lower case) refers to other switches.

1.4 Features

- 24-port 10/100 plus a choice of 4 Gigabit copper or fiber ports
- Supports per-port Egress/Ingress rate control
- Supports 802.3x flow control for Full-duplex mode and collision-based backpressure for half-duplex mode
- Provides trunk groups of up to 8 member ports per trunk
- Broadcast storm prevention
- Supports jumbo frames of up to 9216 bytes
- QoS with 8 Priority Queues
- Embedded 16K MAC address
- Supports STP, RSTP, MSTP
- Tagged VLAN 802.1q with 802.1p up to 4K VLANs

- Supports 802.1X EAP and RADIUS Authentication
- IGMP Snooping V1 / V2 with Multicast Filtering
- Support Layer 3 routing of static route, RIPv1/v2, OSPF
- Support multicast routing DVMRP, PIM-DM
- Support Virtual Router Redundancy Protocol (VRRP)
- Access Control List (Layer 2, 3, 4 and 7)
- QoS Supports 802.1p, WRR, Strict Scheduling Priority Queue, Bandwidth Management
- SNMP V1, V2C, V3 with RMON groups 1, 2, 3 & 9
- FCC Class A & CE approved

1.5 Specifications

Performance:

Throughput:	14,880 packets per second (pps) to 10 Mbps ports
	148,800 pps to 100Mbps ports
	1,488,000 pps to 1000Mbps ports
Address Table Size:	16K MAC entries
Buffer Memory:	32MB
Flash Memory:	8-16MB
VLANs:	Port-based
	Tag-based (4096VLANs)
Link Aggregation:	Max. 8 ports can be combined into a fat pipe
Max. Distance:	UTP: 100 meters
Fiber:	Based on Mini GBIC module
Management via:	SNMP V1, V2C, V3
	Web Management
	Command Line Interface (CLI)
	RS-232 console

Connectors and Cabling:

Ports:	24 x Ethernet/Fast Ethernet ports
	4 x Gigabit Ethernet ports / 4 x Gigabit fiber slots (SFP)

Smart Control: RS-232

SNMP Standards & Protocols:

RFC 1213	MIB II
RFC 1493	Bridge MIB
RFC 1643	Ethernet Interface MIB
RFC 1757	RMON
RFC 1112/2236	IGMP Snooping v1, v2
RFC 1541/2131	DHCP
RFC 1350	TFTP

Network Management:

System Configuration:	Console port, Telnet, Web browser, SNMP/RMON
Management Agent:	SNMP Support: MIB II, Bridge MIB, Ethernet MIB, RMON MIB
RMON Groups:	1, 2, 3, 9 (Statistics, History, Alarm and Event)
Spanning Tree Algorithm:	IEEE 802.1D, 802.1w and 802.1s provide redundant link support
Port-based or 802.1Q VLANs:	Up to 4096 VLANs, with GVRP for dynamic VLAN registration
Link Aggregation:	2~8 ports can be combined into a fat pipe

Standards and Compliance:

IEEE 802.3	10BASE-T
IEEE 802.3u	100BASE-TX and 100BASE-FX
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BASE-SX/LX/LHX
IEEE 802.3ab	1000Base-T
IEEE 802.1p	Priority Queues
IEEE 802.1q	VLAN Tagging
IEEE 802.1D	Spanning Tree Protocol
IEEE 802.1x	Security Protocol
IEEE 802.3ad	Port trunking
IEEE 802.1w	Rapid STP
IEEE 802.1s	Multiple STP

Power Characteristics:

Input voltage:	100 to 240V AC (auto-ranging) 50 to 60 Hz or DC-48V

Power Consumption:	40-Watts max.
Redundant Power:	Redundant power option available

Environmental Characteristics:

Operating	Temperature: 0°C to 50°C
	Relative Humidity: 10% to 80%, non-condensing
Storage	Temperature: -20°C to 80°C
	Humidity: 5% to 90% (non-condensing)

Dimensions:

184 x 440 x 44mm (D x W x H)

Weight:

4kg

Mounting:

Standard 19" Rack-mountable case

Electromagnetic Compatibility:

Emissions: FCC Class A, & CE approved

2 Hardware Description

The NSH-580 is a high-performance managed SNMP Layer 3 switch that provides users with 24 x 10/100Mbps Ethernet and 4 Gigabit Combo ports. The Web/SNMP management provides remote control capability that gives user-friendly and flexible network management and monitoring options.

For increased bandwidth applications, the NSH-580 can accommodate trunk groups with 8 ports in each trunk.

Moreover, these trunk ports ship with fair-over function to provide redundant back-up if one or more of the ports are malfunctioning. It also supports both Port-based VLAN and Tag-based VLAN, thereby simplifying network traffic segmentation, broadcast domain extension and other associated benefits of constructing VLANs. This abundance of features translates into increased efficiency and performance in network administration.

The Switch was especially developed with a host of features that make it particularly suited for SOHO applications which demand the utmost in reliability. The device comes with 24 x 10/100Base-TX copper ports and 4 SFP fiber gigabit ports that are each interchangeable with 4 additional Gigabit Ethernet ports. The package provides 10/100Base-TX copper and Gigabit fiber conversion. Thus, the Gigabit fiber and copper ports provide flexible, high-bandwidth and fast uplinks, while the 10/100TX copper ports offer flexibility in network configurations.

Being SNMP-ready, the Switch enables network managers to remotely monitor the entire network status quickly and easily via RJ-45 (in-band), or console port (out-of-band) connection. This managed Switch can extend the enterprise LAN configuration range up to 110km while simultaneously minimizing the troubleshooting time. The Switch is designed for 'plug-n-play' to enable hassle-free integration in today's managed mixed cabling network configurations.

Featuring auto MDI/MDI-X detection for direct connections to a workstation, switch or hub, network managers no longer need to worry about the cable configuration (crossover or straight through) when establishing connections between RJ-45 ports.

The Switch has auto-negotiation capabilities that allow it to support connection with leading NWay switches. In full-duplex mode, this unit can sustain distances of up to 550m (with multi-mode fiber) and 110km (with long-haul single-mode fiber) between a LAN switch and another switch or data/file server.

2.1 Product Illustration

Front view:

2.2 Connectors

The Switch utilizes ports with copper and SFP fiber port connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.

2.2.1 10/100Base-TX Ports

The 10/100BASE-TX ports support network speeds of either 10Mbps or 100Mbps, and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true “plug-n-play” capability – just plug the network cables into the ports and the ports will adjust according to the end-node devices. The following are recommended cabling for the RJ-45 connectors: (1)10Mbps – Cat 3 or better; (2)100Mbps – Cat 5 or better.

2.2.2 10/100/1000Base-T Ports

The Switch has four Gigabit 10/100/1000Base-T ports for RJ-45 connectors that have the same features as the above-mentioned 10/100 ports. The only difference is that the Gigabit copper ports support network speeds of 10/100/1000Mbps.

These four ports are located next to the four SFP-type fiber slots and each one of these RJ-45 ports is interchangeable with a corresponding SFP slot. The Gigabit copper port will have the same number as its corresponding SFP slot. This means that once an SFP slot is connected, the correspondingly numbered RJ-45 port (25, 26, 27 or 28) will not function.

2.2.3 SFP slots for SFP modules

The four SFP slots are designed to house Gigabit SFP modules that support network speeds of 1000Mbps. These slots are interchangeable with the four 1000Base-T ports to their left and the slots have the same port numbers as their corresponding 1000Base-T ports. This means that once an SFP slot is connected via an SFP module, the correspondingly numbered 1000Base-T port (25, 26, 27 or 28) will not function.

3 Installation

The location chosen for installing the Switch may greatly affect its performance. When selecting a site, we recommend considering the following rules:

- Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- Leave at least 10cm of space at the front and rear of the unit for ventilation.
- Affix the provided rubber pads to the bottom of the Switch to protect the case from scratching.

3.1 Desktop installation

Follow the instructions listed below to install the Switch in a desktop location.

1. Locate the Switch in a clean, flat and safe position that has convenient access to AC power.
2. Affix the four (4) self-adhesive rubber pads to the underside of the Switch.
3. Apply AC power to the Switch (The green PWR LED on the front panel should light up).
4. Connect cables from the network partner devices to the ports on the front panel (The green LNK LED on the front panel associated with the port should light).

This Switch can also be mounted on a vertical surface. Simply use the underside of the unit as a template to measure and mark out the position of the holes on to the surface where the unit is to be installed. Then use the two screws provided to mount the Switch firmly in place.

Warning: Because invisible laser radiation may be emitted from the aperture of the port when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.

3.2 Mounting on a rack

Attach brackets to each side of the switch and place the brackets in the rack's slots. Insert and tighten two screws to securely attach the bracket to the rack on each side.

3.3 Getting Connected

The Switch is capable of connecting up to 28 network devices employing a combination of twisted-pair and fiber cabling paths at Ethernet, Fast Ethernet, or Gigabit Ethernet speeds.

3.4 Powering On the Unit

The Switch uses an AC power supply 100~240V AC, 50~60 Hz, or DC -48V. The power on/off switch is located at the rear of the unit, adjacent to the AC power connector and the system fans. The Switch's power supply automatically self-adjusts to the local power source and may be powered on without having any or all LAN segment cables connected.

1. Insert the power cable plug directly into the receptacle located at the back of the device.

2. Plug the power adapter into an available socket.

Note: For international use, you may need to change the AC power adapter cord. You must use a power cord set that has been approved for the receptacle type and electrical current in your country.

3. Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

3.5 Installing the SFP modules and Fiber Cable

1) The NSH-580 has 4 Gigabit SFP slots situated under the RS-232 port:

2) Slide the selected SFP module into the selected SFP slot. (Make sure the SFP module is aligned correctly with the inside of the slot):

3) Insert and slide the module into the SFP slot until it clicks into place:

4) Remove any rubber plugs that may be present in the SFP module's mouth.

5) Align the fiber cable's connector with the SFP module's mouth and insert the connector:

6) Slide the connector in until a click is heard:

7) If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.

To properly connect fiber cabling: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

> **Note: When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.**

Check the corresponding port LED on the Switch to be sure that the connection is valid. (Refer to the LED chart)

3.6 Connecting Copper Cable

The 10/100BASE-TX RJ-45 Ethernet port fully supports auto-sensing and auto-negotiation.

1. Insert one end of a Category 3/4/5/5e (see recommendation above) type twisted-pair cable into an available RJ-45 port on the Switch and the other end into the port of the network node.

2. Check the corresponding port LED on the Switch to ensure that the connection is valid. (Refer to LED chart)

3.7 Connecting the Console Port Cable

The console port (DB-9) provides the out-of-band management facility.

1 Use null modem cable to connect the console port on the Switch and the other end into the COM port of the computer.

2 Configure the Hyper Terminal settings as mentioned in chapter 5 or 6.3.1.

3.8 Connecting to computers or a LAN

You can use Ethernet cable to connect computers directly to the switch ports. You can also connect hubs/switches to the switch ports by Ethernet cables. You can use either the crossover or straight-through Ethernet cable to connect computers, hubs, or switches.

Use a twisted-pair Category 5 Ethernet cable to connect the 1000BASE-T port, otherwise the link speed will not be able to reach 1Gbps.

3.9 Power On the Unit

Connect the AC power cord to the POWER receptacle on the back of the Switch and plug the other end of the power cord into a wall outlet or a power strip.

Check the front LED indicators with the description in the next chapter. If the LEDs light up as described, the Switch's hardware is working properly.

4 LED Indicators

This Switch is equipped with Unit LEDs to enable you to determine the status of the Switch, as well as Port LEDs to display what is happening in all your connections. They are as follows:

Unit LEDs		
LED	**Condition**	**Status**
POST	Flashing	Indicating POST function upon start-up
	On	POST function successfully performed
PWR1	On (Green)	Primary power normal
	Off	Primary power off or failure
PWR2	On (Green)	Backup power normal
	Off	Backup power off or failure
Port LEDs		
LED	**Condition**	**Status**
10/100 (Copper Ports)	On (Green)	Port operating at 100Mbps
	Off	Port operating at below 100Mbps
LNK/ACT	On (Green)	Illuminated when connectors are attached
	Flashing (Green)	Data traffic passing through port
	Off	No valid link established on port
A (25th~28th Gigabit Ethernet Ports)	On (Green)	Illuminated when connectors are attached
	Flashing (Green)	Data traffic passing through port
	Off	No valid link established on port
B (25th~28th G E Ports)	On (Green)	Port operating at **10Mbps**. If LED C is **also** on, Port is operating at **1000Mbps**.
	Off	If LED C is on, port operating at 100Mbps; or else link down
C (25th~28th G E Ports)	On (Green)	Port operating at **100Mbps**. If LED B is **also** on, Port is operating at **1000Mbps**.
	Off	If LED B is on, port operating at 10Mbps; or else link down

5 Management options

This system may be managed out-of-band through the console port on the front panel or in-band by using Telnet. The user may also choose web-based management, accessible through a web browser.

5.1 Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a web browser.

5.2 SNMP-Based Management

You can manage the Switch with SNMP Manager software. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

5.3 Configuring the Switch via Console Port (RS-232 DCE)

Prior to accessing the switch's onboard agent via a network connection, you must first configure it by giving it a valid IP address, subnet mask, and default gateway, using an out-of-band connection or the BOOTP protocol.
After configuring the Switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network or via internet. The onboard configuration program can be accessed by using Telnet from any computer attached to the network. It can also be managed with any computer using a Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above).
Access the Switch via a terminal emulator (such as Hyper Terminal) attached to the console port. The console port is set at the factory with the following default COM port properties. Configure your own terminal to match the following:

- Baud rate: 38,400
- Data size: 8bits
- Parity: None
- Stop bits: 1
- Flow Control: None

NOTE: Ensure that the terminal or PC you are using to make this connection is configured to match the above settings. Otherwise the connection will not work.

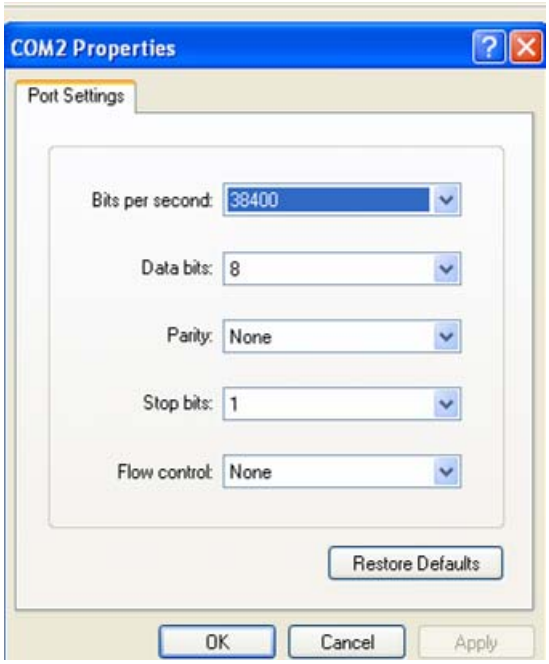
A console port cable is provided with the Switch to connect the PC's COM port with the Switch's serial console (RJ-45) port.

5.3.1 Using HyperTerminal to Set IP address

Prior to following the instructions listed below for HyperTerminal, verify that a console cable (RJ45 to DB9) connection between the Switch and workstation exists. Then follow the steps below:

1. Launch the terminal emulation program on the remote workstation and power on the Switch. Be sure to select the correct COM port.

2. Enter the correct parameters according to the defaults given on the previous page:



3. The prompt screen will appear after selecting “OK”. The default log-in name is “admin” with no preset password (just press <ENTER>).

4. The prompt **Switch>** will appear. For a list of main commands, type “?” and <Enter>. For a list of sub-commands, type a main command like “list” and <Enter>:

```
Switch>
  enable      Turn on privileged mode command
  exit        Exit current mode and down to previous mode
  list        Print command list
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
  web_pass    internal use only
Switch> list
```

After successful log-in, type the following command line to change the device IP, Network Mask, and Gateway address:

```
Switch#config terminal
Switch(config)#interface vlan1
Switch(config-if)#ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
Switch(config-if)#exit
Switch(config)#ip route 0.0.0.0/0 xxx.xxx.xxx.xxx
```

The **xxx**s represent values between **0** and **255** and the user should enter their own IP address in this form. The configuration program will not accept anything outside this format. Remember to separate each part of the address with a period (dot).

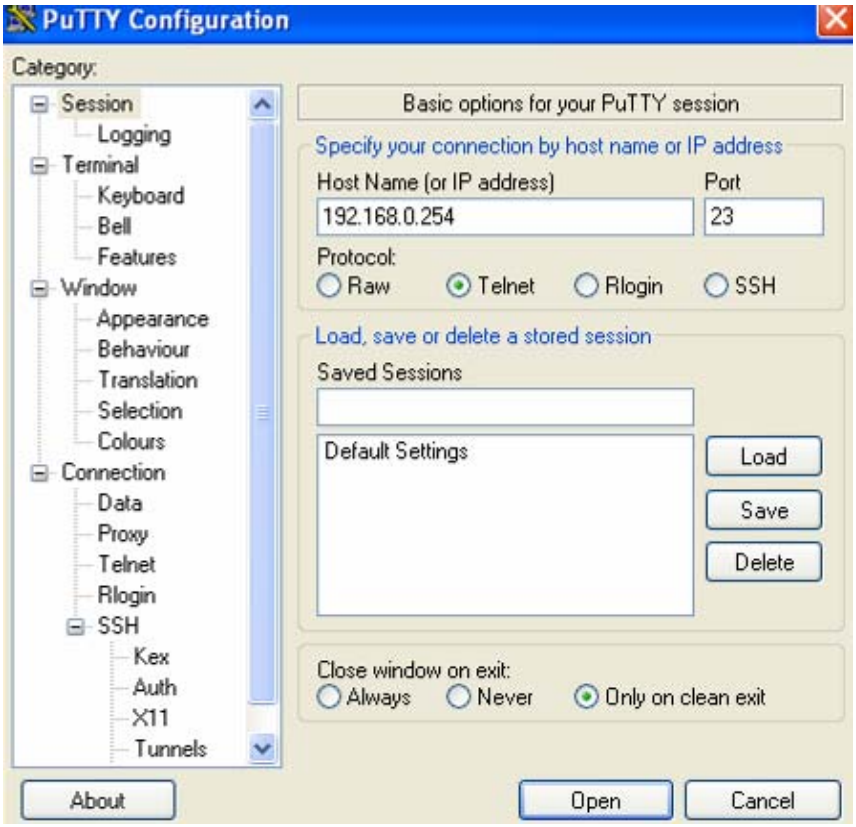
When the address has been changed, please make a note of the new address, and keep it in a safe place. With HyperTerminal, the command lines are the same as that for telnet. Users can continue to use Hyper Terminal along with the instructions given in next sections. Otherwise, log out by typing 'exit' and pressing the <**ENTER**> key. Then, the user can choose to configure the Switch via HTTP Web Browser or Telnet with Menu Driven or Command Line interfaces.

Note: *IP addresses are unique. If an address isn't available, please contact the appropriate authorities to apply for one.*

5.4 Telnet and SSH

Activate your workstation's command prompt program (like Putty) and access your Switch via the Internet by typing in the correct IP address (factory default IP address is 192.168.0.254 – connect directly via console port to configure a unique IP address). A command prompt program like Putty will give you the option of choosing either Telnet or SSH (Secure Shared) protocol. SSH is an encrypted protocol and is ideal for ISP workers who have to be extra careful when managing their switches.

Figure underneath: Screenshot of Putty program where IP address is typed in and Telnet or SSH is selected:



After opening the program, a command prompt screen will appear. At the **Switch login** line, type the pre-set password – the factory default is **admin**. Type '**?**' for a list of main commands. On the screenshot below, the writer had typed the **list** command below the last listed main command.

```
Switch login: admin

Switch>
  enable       Turn on privileged mode command
  exit         Exit current mode and down to previous mode
  list         Print command list
  ping         Send echo messages
  quit         Exit current mode and down to previous mode
  show         Show running system information
  telnet       Open a telnet connection
  traceroute   Trace route to destination
  web_pass     internal use only
Switch> list
  enable
  exit
  list
  ping WORD
  ping ip WORD
  quit
  show arp
  show gvrp statistics [IFNAME]
  show ip forwarding
  show ip ospf
```

5.5 SNMP Settings

Simple Network Management Protocol (SNMP) is an Application Layer designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network. Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

5.6 Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

5.7 MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. MIB values can be either read-only or read-and-write.

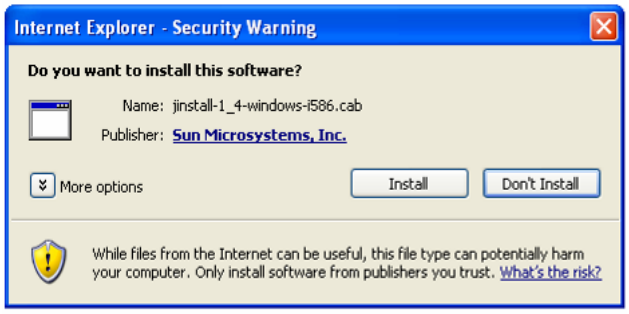
6 First Time Connecting to the Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells you how to log into the Switch.
If you don't have the correct version of Java on your computer, the following will apply to you:

INSTALLING the Java Runtime Environment Software:
If you don't already have the correct Java Runtime Environment (JRE) on your computer, this guide will help you to install it. To test if you already have the correct software, open your network browser (**you must be connected to the internet for the following function**) and type in the factory default IP address of the Switch: **192.168.0.254** in the address bar. If a pop-up screen appears and advises you to click on it to install, do so.

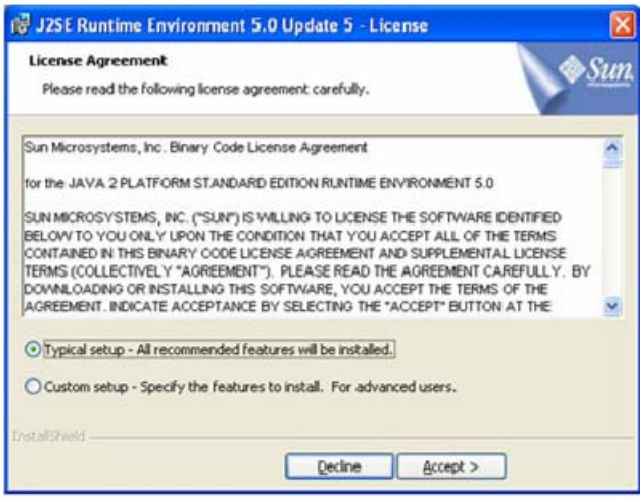
NOTE: Depending on your connection speed, this process will take between 5 to 30 minutes to complete.

Step 1: If you get this 'security warning', click "Install".

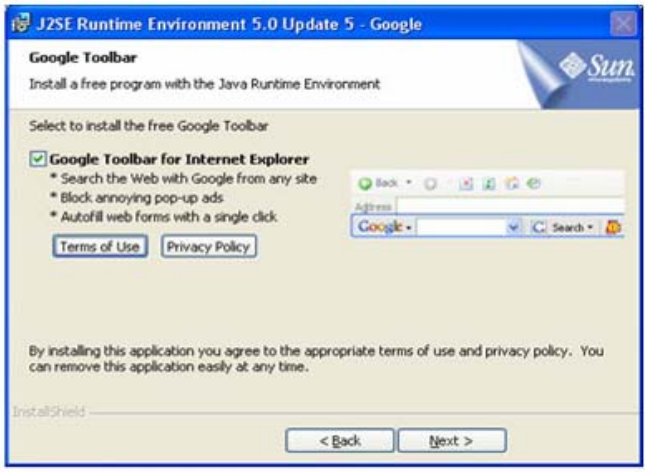

Internet Explorer - Security Warning
Do you want to install this software?
Name: jinstall-1_4-windows-i586.cab
Publisher: Sun Microsystems, Inc.
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Step 2: The installation page will appear. Wait until the next screen appears.

Step 3: This is the User's Agreement page. Read through it and click on the "I Agree" button. (The page also gives you the option to choose "Typical setup" or "Custom setup".
(The software vendor strongly suggests that the user selects option 1 – Typical.)

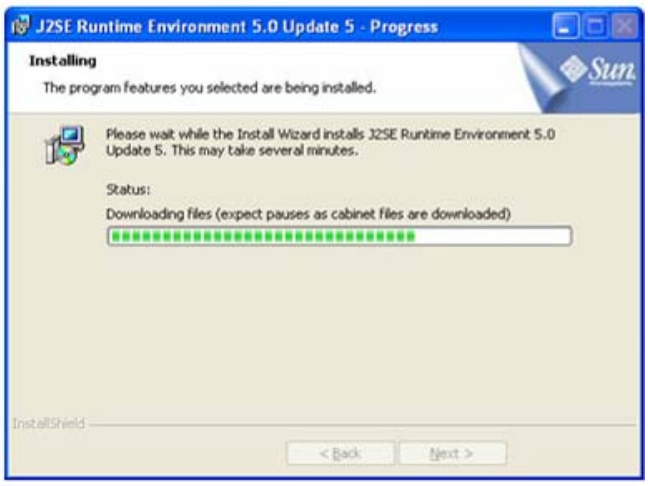

J2SE Runtime Environment 5.0 Update 5 - License
License Agreement
Please read the following license agreement carefully.
Sun Microsystems, Inc. Binary Code License Agreement
for the JAVA 2 PLATFORM STANDARD EDITION RUNTIME ENVIRONMENT 5.0
SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE
Typical setup - All recommended features will be installed.
Custom setup - Specify the features to install. For advanced users.
InstallShield
Decline
Accept >

Step 4: If Internet Explorer is set as the default browser on your system, then the Java Runtime Environment 5.0 Update 5 – Google Programs dialog box will appear. By default, Google Toolbar for Internet Explorer is checked. Click the "Next" button. This will start installing selected program features, including the JRE, on your system.


J2SE Runtime Environment 5.0 Update 5 - Google
Google Toolbar
Install a free program with the Java Runtime Environment
Select to install the free Google Toolbar
Google Toolbar for Internet Explorer
* Search the Web with Google from any site
* Block annoying pop-up ads
* Autofill web forms with a single click
Terms of Use
Privacy Policy
By installing this application you agree to the appropriate terms of use and privacy policy. You can remove this application easily at any time.
InstallShield
< Back
Next >

Note: You can choose to install or ignore this useful additional program by checking or un-checking the check box.

Step 5: This page appears when the installation process has started and shows you how far the process has progressed. Depending on your connection speed, the process can take between 5 and 30 minutes.


J2SE Runtime Environment 5.0 Update 5 - Progress
Installing
The program features you selected are being installed.
Please wait while the Install Wizard installs J2SE Runtime Environment 5.0 Update 5. This may take several minutes.
Status:
Downloading files (expect pauses as cabinet files are downloaded)
InstallShield
< Back
Next >

Step 6: A few brief dialog boxes will confirm the last steps of the installation process, and a concluding message will appear with the confirmation "Installation Completed OK." Click "Finish".

Step 7: After finishing the installation process, the program will show this page every time you type the IP address. **The default User Name and Password is "admin" and "admin".**
Click OK to enter the management interface of the NSH-580.

TROUBLESHOOTING: If you still have problems accessing the hyperlink, check the following:
1) Check the firewall in your PC or the firewall that your company uses. This firewall could be blocking access to the hyperlink.
2) Make sure you have downloaded the latest version of Java Runtime Environment. This software will run on any of the normal Windows systems, as well as on Unix.

7 Web Management

The Switch provides Web pages that allow equipment management through the Internet. The Java Runtime Environment (JRE) is required to run Java applet programs that are automatically downloaded from the Switch during management functions. (See section 7 above).

7.1 Log into Web Management

From a PC, open your web browser, type the following in the web address (or location) box: http://192.168.0.254 and then press <Enter>. This is the factory default IP address for the switch. A login screen is displayed, as shown in the figure on the right:

Configuration manager login screen:

Enter your user name and password, then click OK.
Use the following defaults the first time you log into the program. You can change the password at any time through CLI interface (see section 6.3.1).

Default User Name: admin
Default Password: admin

The **home page** appears each time you log into the program. See figure **below**:
The meanings of the green and orange buttons are further explained in the next section.

VOLKTEK
Config Menu
System
Physical Interface
IP Interface
Router Reports
Routing
Bridge
SNMP
ACL
Security
Traffic Chart
Save Configuration
Welcome to Switch manager
Web GUI
Submit
Submit the edited settings on the browser page to the Switch to be effective.
Refresh
Refresh the displayed settings from the Switch.
New
Create a new provisional record for user to edit the settings on browser page for adding to the indexed table.
Add
Add the edited provisional record to the table of the browser page to be submitted.
Modify
Modify the highlighted record of the table on the browser page with the edited provisional data.
Remove
Remove the highlighted record of the table from the browser page.
Detach All
Detach all ports from the settings like VLAN, port mirroring, etc.

7.1.1 Standard GUI buttons

Click **New** to create a new entry for editing to the table (temporary until **Submit** is clicked).

Click **Add** to add the new entry to the table (temporary until **Submit** is clicked).

Click **Modify** to temporarily save changes to an existing entry (temporary until **Submit** is clicked).

Click **Remove** to remove selected entry (temporary until **Submit** is clicked).

Click **Attach All** to select all ports for a selected entry (temporary until **Submit** is clicked).

Click **Detach All** to unselect all ports for a selected entry (temporary until **Submit** is clicked).

Click **Submit** to save changes to RAM memory of the Switch.

Click **Refresh** to display current settings of the Switch for viewing the effect of changes.

To eventually make all changes permanent in Flash memory of the Switch, go to "**Save Configuration**" **page** (bottom of management menu) and click **Save**. **Submit** only configures the Switch hardware and saves the settings to RAM memory and such changes will be lost if the Switch is powered off.

Warning

Clicking **Submit** only saves the information to the Switch's RAM memory and **changes will still be lost if the Switch is powered off**. To save changes permanently in the Switch's Flash memory, click on the "**Save Configuration**" button of the Switch's management menu. Once the "**Save Configuration**" **page** appears, click **Save** to store all configurations in Flash memory permanently.

7.2 System

System pages include Management, IP Setup, Reboot, and Firmware Update function.

7.2.1 Management

The **Management** page contains the following information:

Model Name: product name

MAC Address: Switch MAC address

System Name: user-assigned name to identify the system (editable)

System Contact (editable)

System Location (editable)

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To eventually make all changes permanent in Flash memory, go to **"Save Configuration" page** (bottom of management menu) and click **"Save"**.

Management Page

Warning The character '!' and '#' cannot be used as or inside the text string value of any attribute, no matter it's configured through Web Management or Command Line Interface. For example, "Switch!" or "#Switch" is not a valid System Name.

7.2.2 IP Setup

The IP Setup page contains the following information:

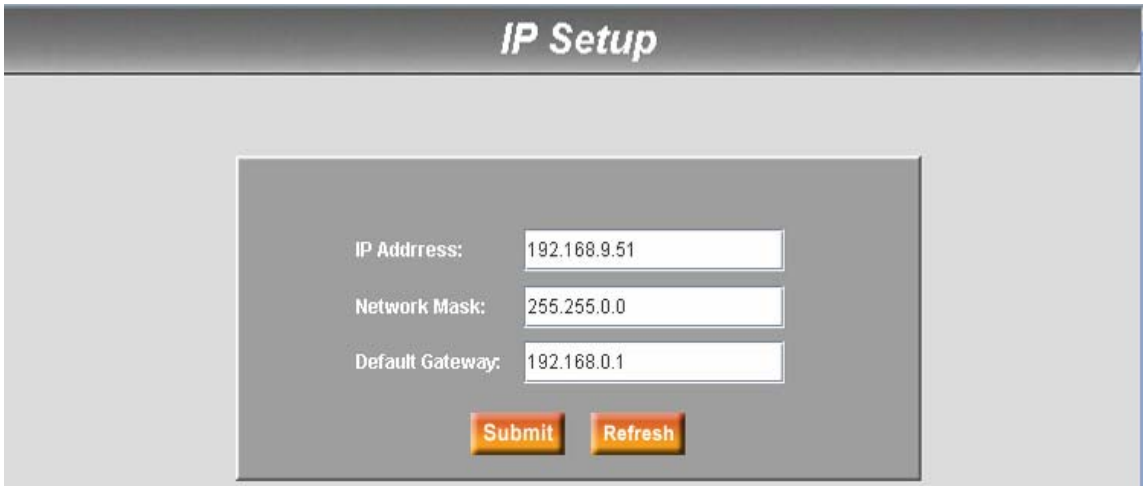
IP Address: IP address for the switch

Network Mask: Network mask for this network

Default Gateway: Default gateway for this network

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To eventually make all changes permanent in Flash memory, go to **"Save Configuration" page** (bottom of management menu) and click **"Save"**.

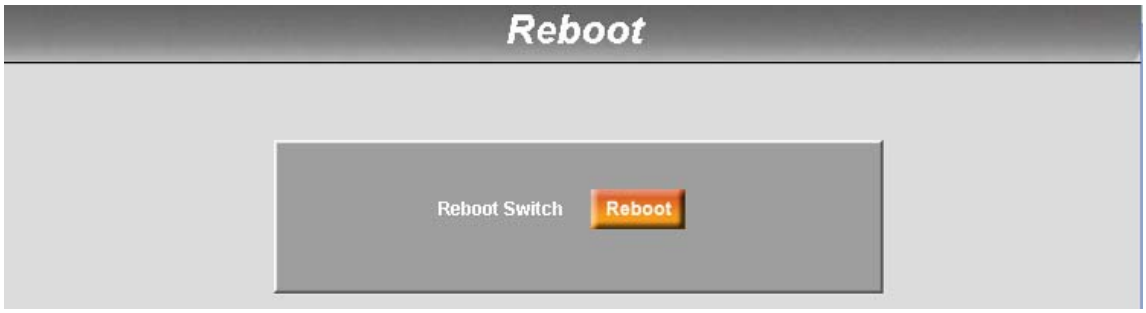


IP Setup Page

7.2.3 Reboot

The Reboot page contains a **Reboot** button. Clicking the button reboots the system.

Rebooting the system stops the network traffic and terminates the Web interface connection.



Reboot Page

7.2.4 Firmware Upgrade

Enter the TFTP server IP address and the firmware file name. Click **Upgrade** to update the Switch's firmware from TFTP server. See figure below for reference. For example,

TFTP Server: 192.168.1.155

File Name: 3112Single-v10.img

Clicking the upload button loads the assigned firmware to the Switch, then reboot system after a successful firmware update. The user will need to log in to the web interface again.

Firmware Upgrade Page

7.3 Physical Interface

7.3.1 Port Status

7.3.1.1 Interface Configuration

The **Physical Interface** displays the Ethernet port status in real time. You can configure the port in the following fields in Interface Configuration Window:

Port: select the port to configure

Status: disable/enable the port

Mode: set the speed and duplex mode

Flow Control: enable/disable 802.3x flow control mechanism

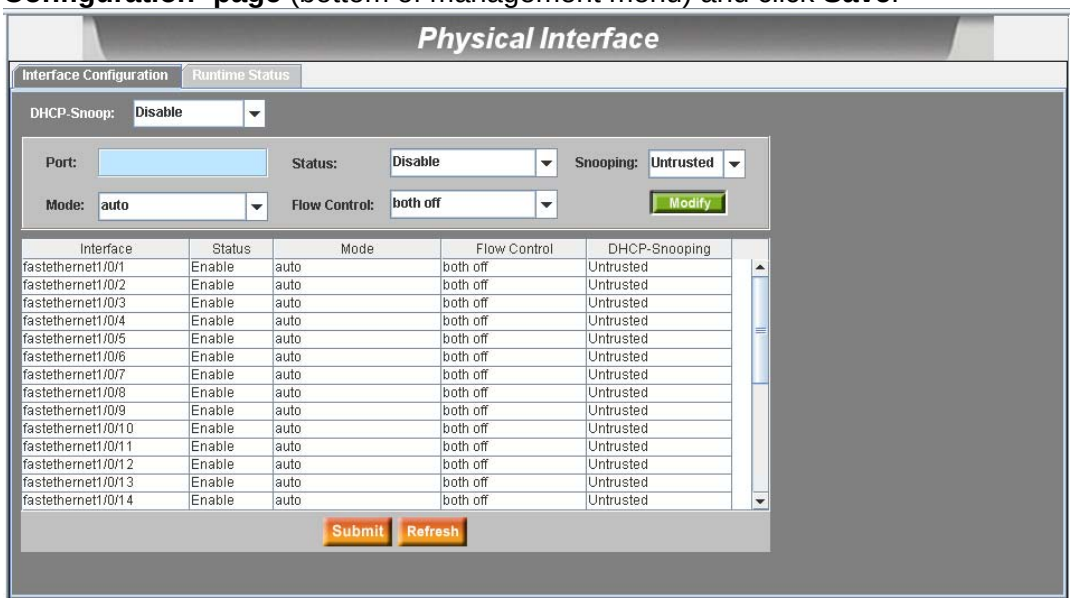
DHCP-Snooping: enable/disable DHCP snooping function

Snooping: assign the selected port to be a trusted or not trusted port

Select the corresponding port number and configure the port setting, then click on the **Modify** button. The field you change will update the content of the display window. However, the new settings do not take effect until the **Submit** button is clicked.

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To eventually make all changes permanent in Flash memory, go to "**Save Configuration**" **page** (bottom of management menu) and click **Save**.



Physical Interface – Interface Configuration

7.3.1.2 Runtime Status

This window displays the following information for each port:

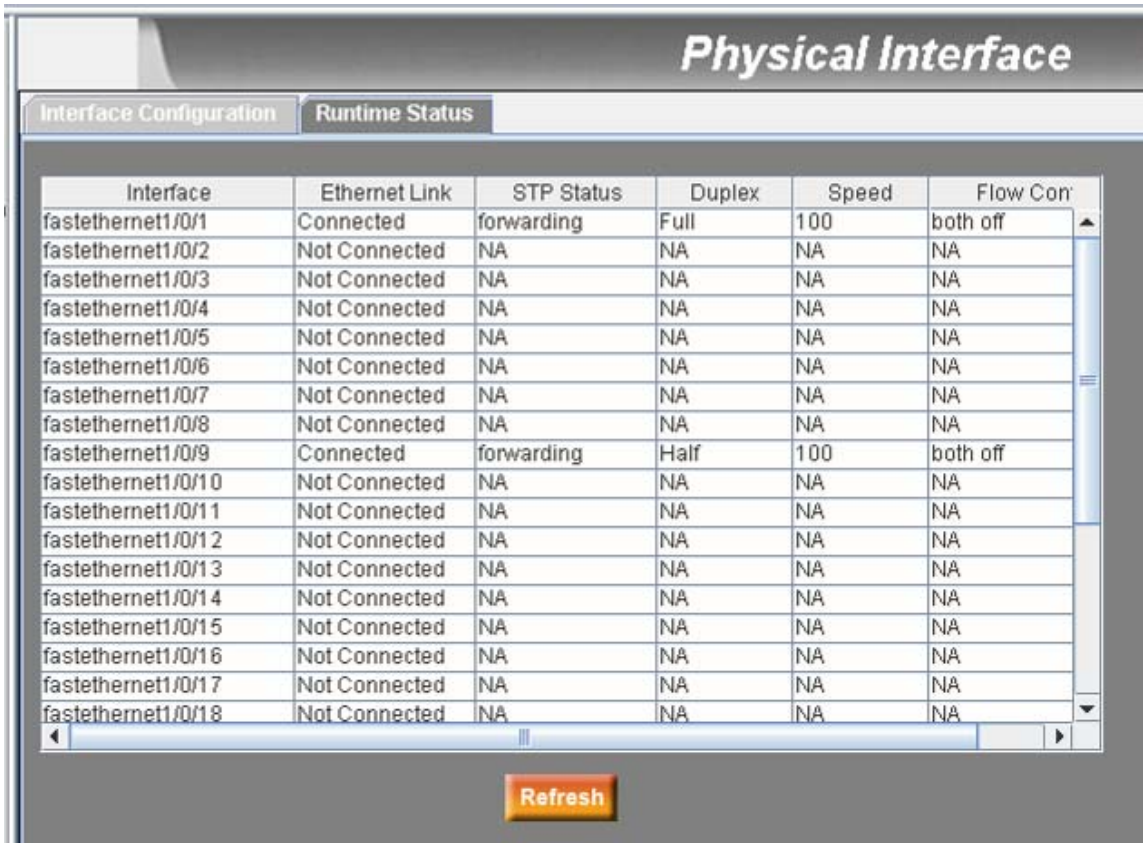
Ethernet Link: the link is connected or not connected.

STP Status: STP is enabled or disabled on the port

Duplex: the duplex mode

Speed: link speed

Flow Control: the setting of 802.3x flow control mechanism on both directions of the port



Interface	Ethernet Link	STP Status	Duplex	Speed	Flow Con
fastethernet1/0/1	Connected	forwarding	Full	100	both off
fastethernet1/0/2	Not Connected	NA	NA	NA	NA
fastethernet1/0/3	Not Connected	NA	NA	NA	NA
fastethernet1/0/4	Not Connected	NA	NA	NA	NA
fastethernet1/0/5	Not Connected	NA	NA	NA	NA
fastethernet1/0/6	Not Connected	NA	NA	NA	NA
fastethernet1/0/7	Not Connected	NA	NA	NA	NA
fastethernet1/0/8	Not Connected	NA	NA	NA	NA
fastethernet1/0/9	Connected	forwarding	Half	100	both off
fastethernet1/0/10	Not Connected	NA	NA	NA	NA
fastethernet1/0/11	Not Connected	NA	NA	NA	NA
fastethernet1/0/12	Not Connected	NA	NA	NA	NA
fastethernet1/0/13	Not Connected	NA	NA	NA	NA
fastethernet1/0/14	Not Connected	NA	NA	NA	NA
fastethernet1/0/15	Not Connected	NA	NA	NA	NA
fastethernet1/0/16	Not Connected	NA	NA	NA	NA
fastethernet1/0/17	Not Connected	NA	NA	NA	NA
fastethernet1/0/18	Not Connected	NA	NA	NA	NA

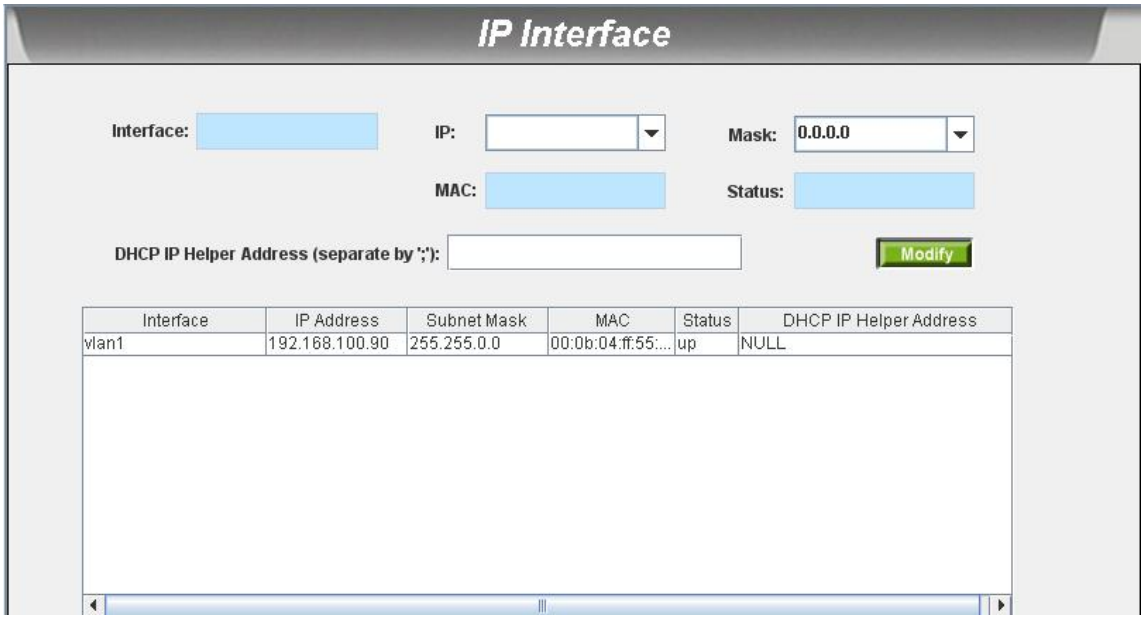
Physical Interface – Runtime Status

7.4 IP Interface

This function allows users to see the **Layer 3** interface status in real time. Users can also configure the interface in the following fields:

Interface: Select the interface to be configured (vlan1 is used by the system).
IP: Interface IP address
Mask: Interface Subnet mask
MAC: Mac address of this interface
Status: up/down status of this interface
DHCP IP Helper Addr: The DHCP Helper Address is the IP address of your DHCP server.
Select the corresponding interface and configure the interface parameters – then click on the button. The field you changed will update the associated content in the display window. To save any changes and make it effective immediately, click **Submit**. Use **Refresh** to refresh the display.

NOTE: There is one more thing to remember regarding DHCP and VLANs. Because each VLAN is a separate IP subnet, you must configure your DHCP server to deliver IP addresses that are appropriate for each subnet. With Windows 2000's DHCP server, you do this by setting up a separate DHCP realm for each VLAN. Not all DHCP servers have this capability. If your existing DHCP server works only with flat LANs, you'll probably have to upgrade to a more sophisticated package.

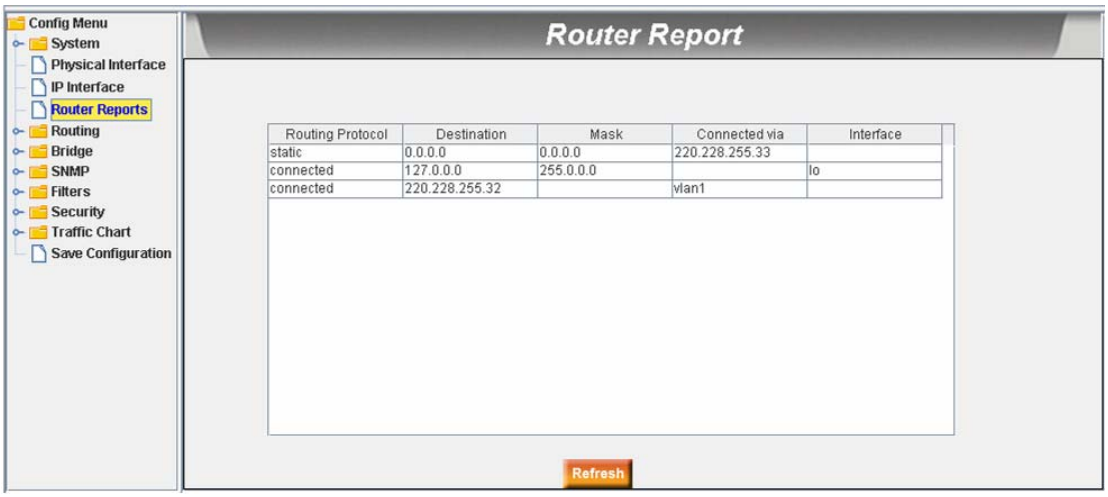


IP Interface

SPECIAL NOTE: It is strongly recommended that each interface should have its own VLAN. That means one VLAN should not be assigned for two interfaces. Otherwise it will create confusion when the RIP is enabled. It is also recommended that only one physical port should be assigned to the VLAN that used for L3 interface. Assigning multiple ports to one L3 interface will result in the L3 traffic going through the port with lowest ID. Traffic load sharing is not supported in this release.

7.5 Router Reports

Router Reports displays the routing table of the Switch.



Router Reports

Routing Protocol: the routing protocol type of the route. If it is "connected", the destination is on the local LAN segment connected to the interface
Destination: destination IP address. It will be masked to generate an IP range as the objective IP addresses of packets to be routed.
Mask: the mask for generating a range of IP addresses.
Connected via: IP address of the next router for routing to another network.
Interface: the interface or VLAN ID from which the packets are routed outside.

7.6 Routing

7.6.1 Static Route

This function is used to add a routing entry into the switch routing table. The routing entry added this way will never be deleted by the system, so it is called a static route. Following parameters must be input to configure static route:

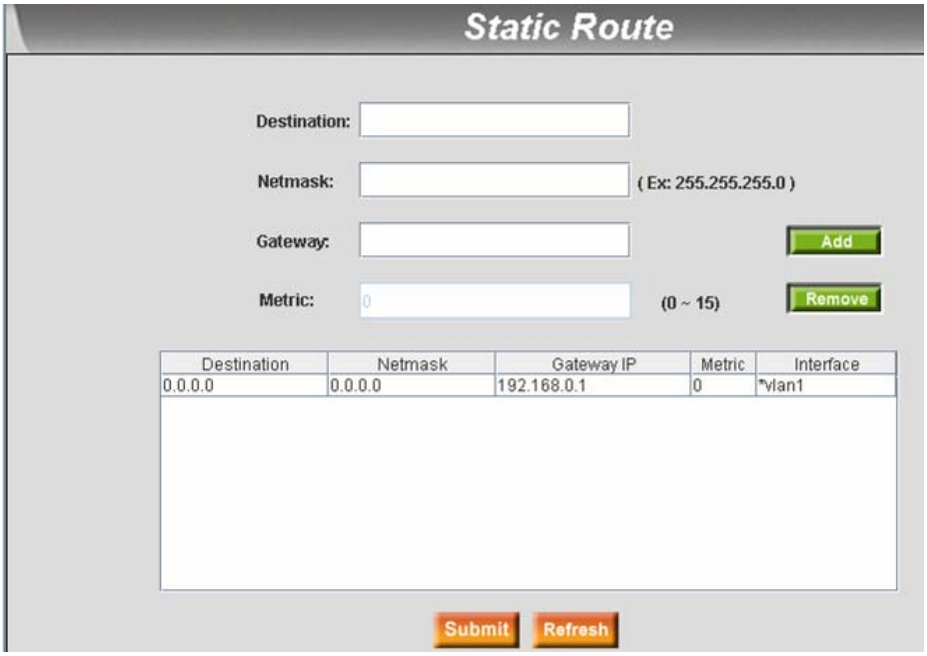
Destination: Input destination IP address.

Netmask: Input subnet mask of the destination for generating the IP range to be routed.

Gateway IP: Input gateway IP address as the next router the packets to be sent to.

Metric: Input metric (1-15). The lower the metric value is the more preference of the route.

Click on **Add** when you add a new static route and you will see the new added entry shows in the list window. You can remove the selected route by clicking **Remove**. The routes that are added or removed will be stored in the configuration file immediately.



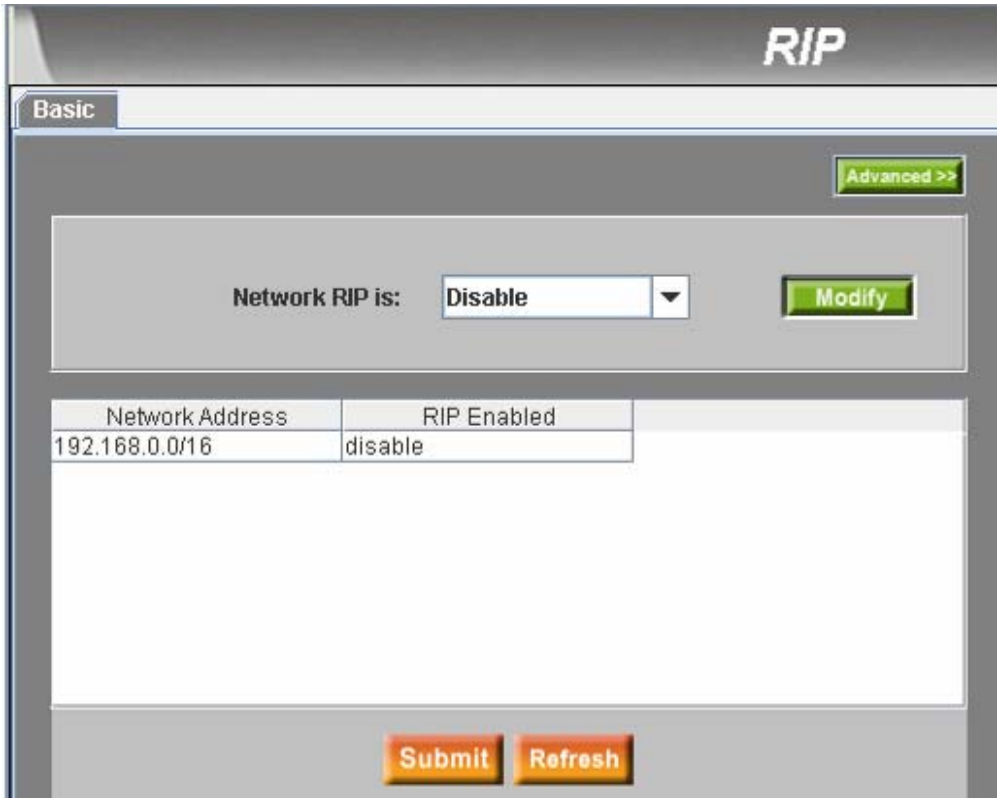
Configure the Static Route

7.6.2 RIP

This function is used to switch on/off RIP routing protocol. Clicking will enable configuration of Passive-Interfaces and RIP version (v1/v2/both). When RIP is turned on, the switch will exchange routing information with neighbor switches which also running RIP.

7.6.2.1 RIP – Basic

The RIP function can be enabled/disabled for all Layer 3 interfaces. All active L3 interfaces will be shown on the screen and the RIP function can be enabled/disabled for each interface. Clicking the **Advanced >>** button will show the other RIP options as discussed in later sections.



Configuring the RIP

7.6.2.2 RIP – Passive Interfaces

If an interface does not need to receive and forward routing updates, the user should disable the sending of routing updates through it. The particular subnet will continue to advise other interfaces of routing updates. Routing updates from other routers on that interface will continue to be received and processed.

Passive Interface: Used to enable/disable the passive interface function for a specific L3 interface. If an interface is enabled as passive, the RIP update messages will not be sent out through it except to RIP neighbors.

7.6.2.3 RIP Version

This L3 switch can support RIPv1, RIPv2 or both.

Incoming Packets: Used to specify RIP version for the interpretation of incoming RIP packets

Outgoing Packet: Used to specify the RIP version for sending RIP packets to neighbor router

7.6.3 OSPF

This function is used to configure the OSPF routing protocol.

7.6.3.1 OSPF – Basic

The user can use this page to add L3 interfaces to specific OSPF areas.

IP Address: All active L3 interfaces are displayed – you can select any one to configure as OSPF interface

Area : Specify the area ID for a specific L3 interface

Clicking the **Advanced >>** button adds extra buttons for “Interfaces” and “Area” options next to the “Basic” button.

OSPF – Basic

7.6.3.2 OSPF – Interfaces

This function is used to specify some protocol parameters for a specific OSPF interface

Network Type: Support broadcast only

Cost: Specify the cost for sending packet of this interface

Priority: Set priority to help determine the OSPF DR and BDR for a network

Transmit Delay: Set the estimated number of seconds to wait before sending a link update packet

Hello Interval: Set the number of seconds between two hello packets, 10 seconds is set as default value

Dead Interval: Set the number of seconds after the last hello packet was received before declare its neighbor OSPF router is down; the default value is 40 seconds.

Retransmit Interval: Specify the number of seconds between transmitting link state advertisements

OSPF – Interfaces

7.6.3.3 OSPF – Area

This function is used to configure OSPF areas

Select an Area: Input area ID to be configured

Default Cost: Default cost for a stub area sending packet to outside world

Stub: a stub area, at the edge of an AS, is not a transit area since there is only one connection to the stub area. Use this attribute to specify characteristics of this area (*no defined* – not a stub area, *no-summary* -- do not inject inter-area routes into stub, and *summary* -- allow injecting inter-area routes into stub)

Shortcut: enable or disable shortcut of the OSPF area (no defined, disable, enable)

OSPF – Area

7.6.4 Multicast Route

This function is used to configure Multicast Route feature. It offers two different methods including DVMRP and PIM-DM to establish multicast route. Also, IGMP will be automatically enabled/disabled with Multicast Route Protocol. It allows hosts to communicate their specific data destined for a specific multicast group. Multicast route protocol uses this information to build and maintain multicast distributed tree.

7.6.4.1 M.R. – IGMP

This command is used to configure the IP multicast route mode and IGMP parameters.

IP Multicast Route Mode: Configure a multicast route protocol to run or disable.

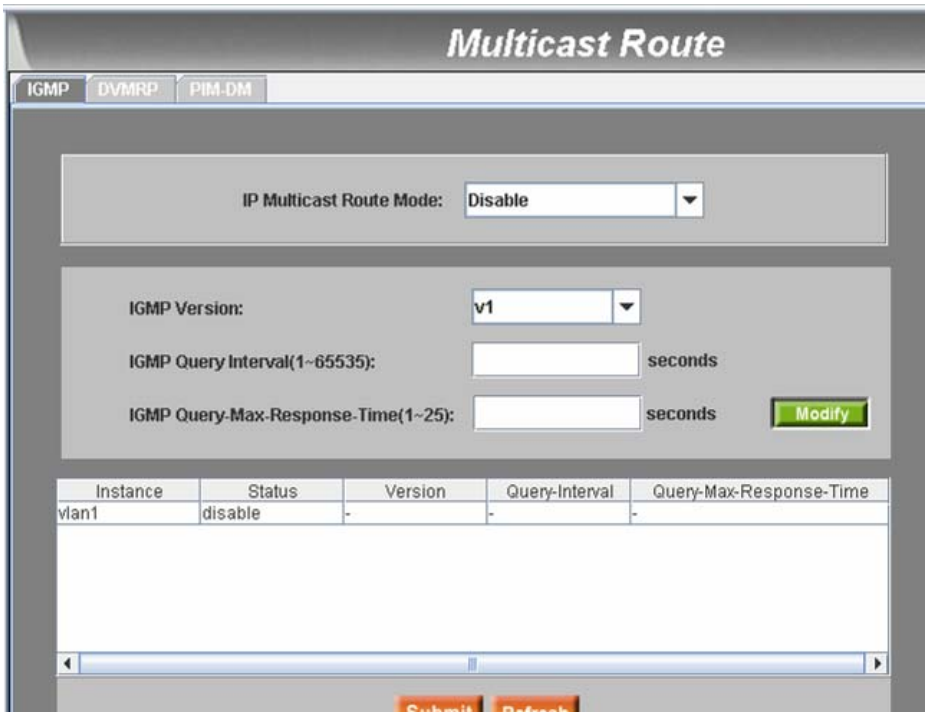
IGMP Version: Select which version of IGMP run. Default value is V2.

IGMP Query Interval: Set the number of seconds between two query packets. Default value is 125 sec.

IGMP Query-Max-Response: Set response time when host reports its multicast group. Default value is 10 sec.

NOTE:

When setting IGMP, select the corresponding interface to configure parameters then click on the **Modify** button. The field you changed will update the content in the display window. To save any changes and make them effective immediately, click **Submit**. Click **Refresh** to refresh the settings.



Multicast Route – IGMP

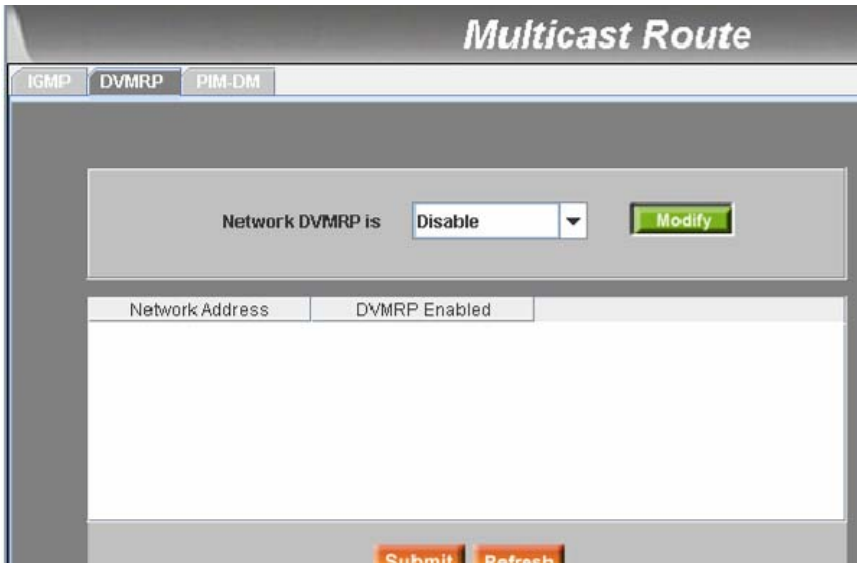
7.6.4.2 M.R. – DVMRP

This function is used to configure DVMRP.

Network DVMRP is: Enable or disable DVMRP for specific network.

Select the corresponding “Network Address” to configure parameters then click on the Modify button. The field you changed will update the content in the display window. To save any changes and make it effective immediately, click **Submit**. Use **Refresh** to refresh the setting.

NOTE: Before setting this page, make sure that the “IP Multicast Route Mode” on the IGMP page is set to “DVMRP”.



7.6.4.3 Multicast Route – PIM-DM

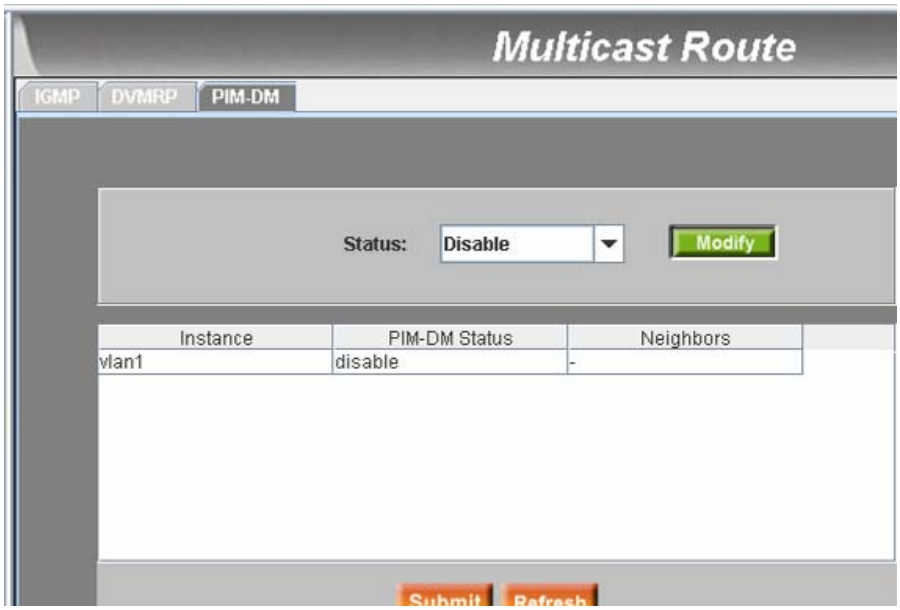
This function is used to configure PIM-DM.

Status: Enable or disable PIM-DM for specific interface.

Select the corresponding interface to configure parameters then click on the Modify button. The field you changed will update the content in the display window. To save any changes and make it effective immediately, click **Submit**. Use **Refresh** to refresh the setting.

NOTE: The system only supports PIM-DM version 2.

NOTE: Before enabling, the “IP Multicast Route Mode” on the IGMP page must be set to “PIM-DM”.



7.6.5 VRRP

The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the weak point inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility, should the Master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end host.

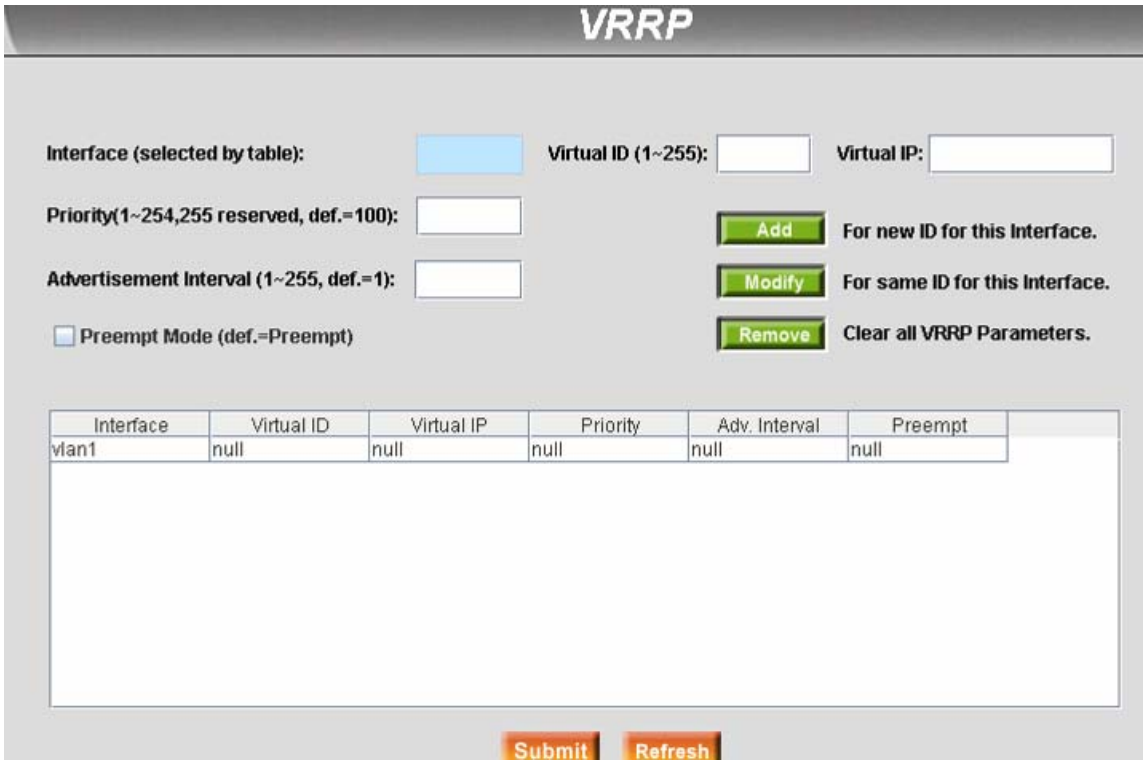
Virtual ID: Virtual router ID, range 1 to 255. One virtual router ID can be used as the default gateway for one or several VLANs.

Virtual IP: Virtual IP address. It can be any one IP address which belongs to the VLAN to be managed. In general, it can be the same as the interface IP address and you expect it to act as master router.

Priority: Virtual router priority. Range 1 to 254, default 100. Higher value means higher priority. Priority value to be used by this VRRP router in selecting the Master for this virtual router. The value of 255 (decimal) is reserved for the router that owns the IP addresses associated with the virtual router. The value of 0 (zero) is reserved for Master router to indicate it is releasing responsibility for the virtual router. The range 1-254 (decimal) is available for VRRP routers backing up the virtual router.

Advertisement Interval: Time interval between ADVERTISEMENTS (seconds). Default is 1 second.

Preempt Mode: Controls whether a higher priority Backup Router preempts a lower priority Master. Values are True to allow preemption and False to not prohibit preemption. Default is True.



VRRP

7.7 Bridge

The Bridge page group contains Layer 2 configurations like link aggregation, STP, etc.

7.7.1 Spanning Tree

This section configures three types of Spanning Tree Protocol.

7.7.1.1 STP Status

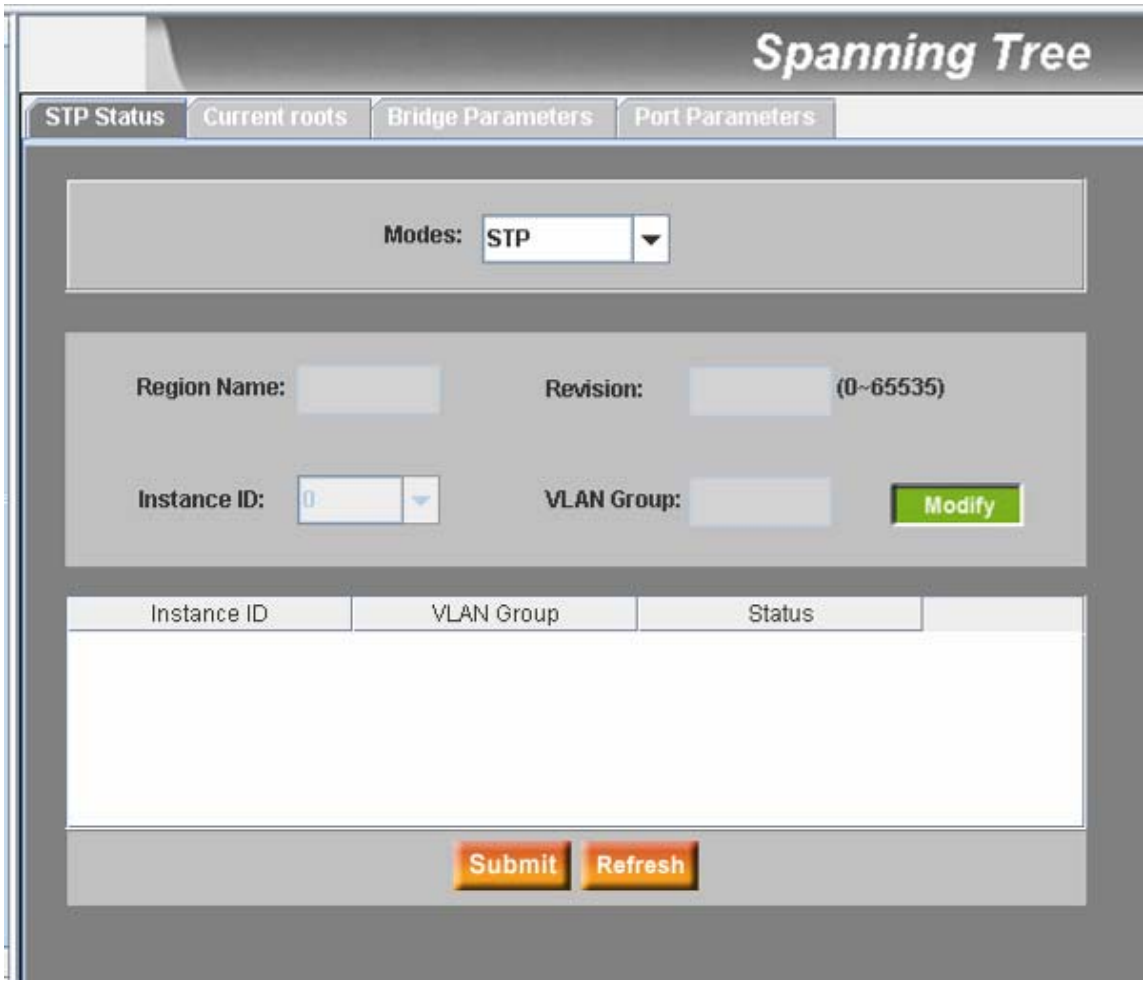
The first page, "**STP Status**", can disable or enable STP. There are three modes of STP, RSTP and MSTP can be enabled. If MSTP is enabled, the following four attributes are enabled at the same time:

Region Name: An alphanumeric configuration name

Revision: A configuration revision number to identify the region along with the Region Name

Instance ID: A STP instance, you can configure MSTP on your Switch to map multiple VLANs into a single STP instance.

VLAN Group: A group associates each of the potential 4094 VLANs to the given instance.



Spanning tree – STP Status

7.7.1.2 Current Roots

This shows the information of the current root bridge, which includes:

MAC Address of root bridge

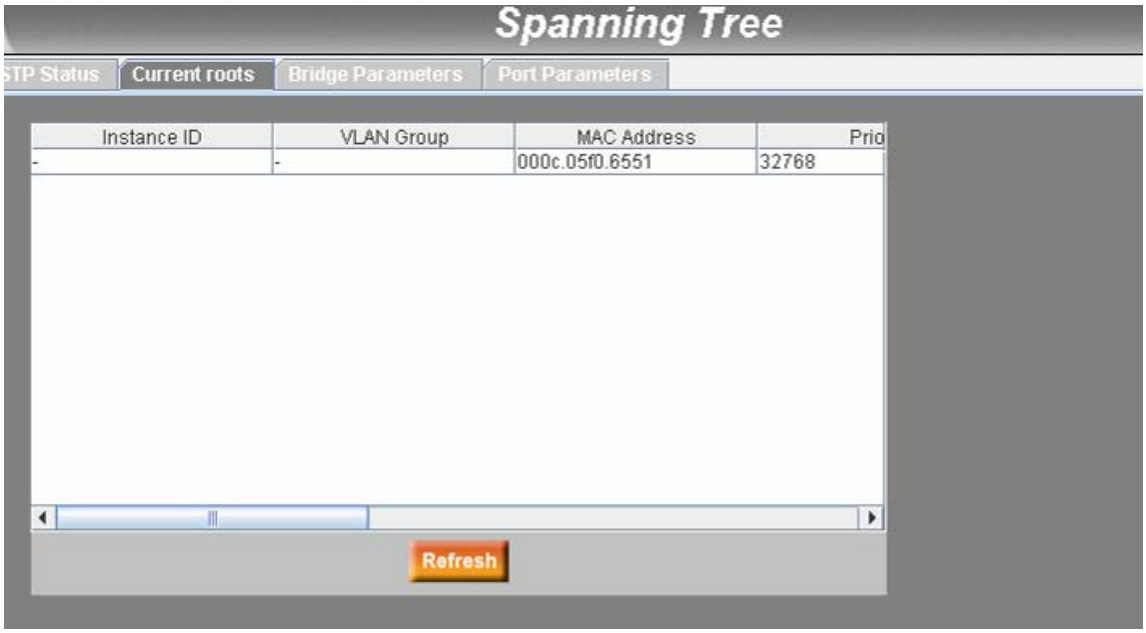
Priority of root bridge

Maximum age of root bridge

Hello timer of root bridge

Forwarding delay timer of root bridge

Path cost of root bridge



Spanning tree – Current Roots

7.7.1.3 Bridge Parameters

The spanning-tree parameters of BPDU transmission can be configured on this panel:

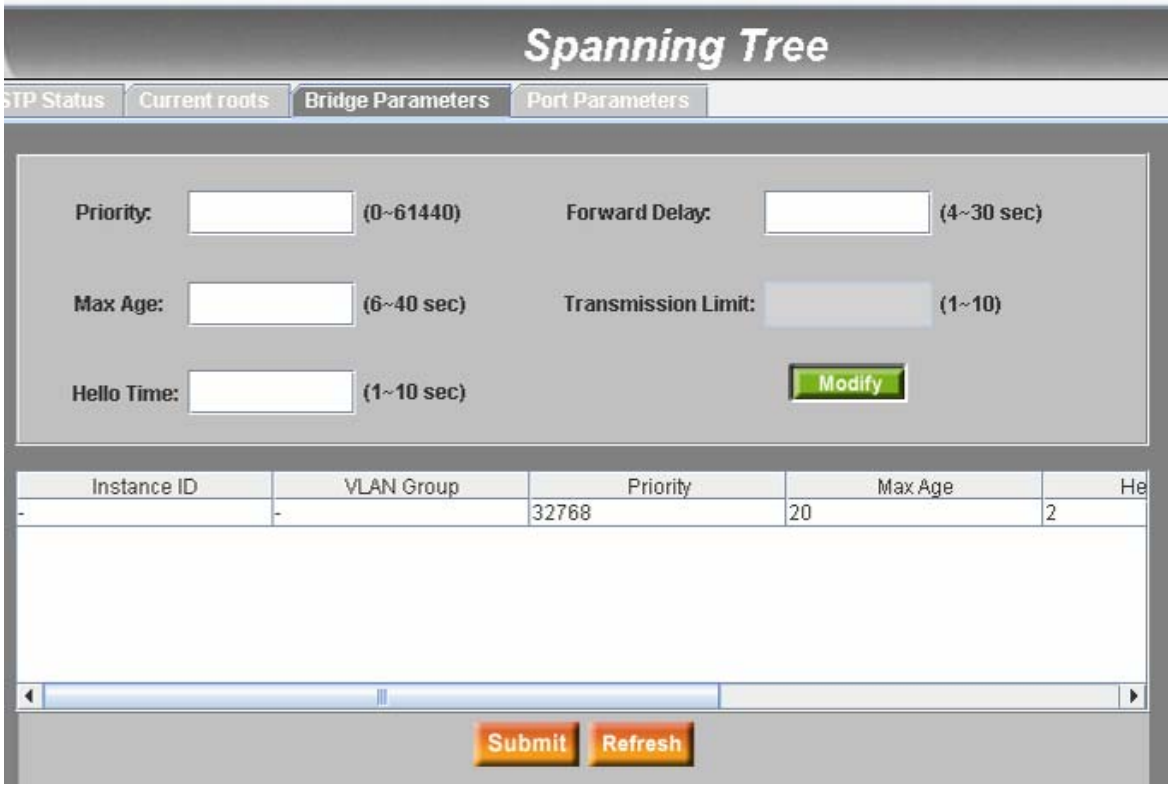
Hello Time: the interval between the generation of configuration BPDU

Max Age: a timeout value to be used by all Bridges in the LAN

Forward Delay: a timeout value to be used by all bridges in the LAN

Bridge Priority: the switch priority in the LAN

Transmission Limit: The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the transmission limit set to the maximum value.



Spanning tree – Bridge Parameters

7.7.1.4 Port Parameters

This page contains a display window to show and edit the current configurations for each port. You can select a port then edit it. Click **Modify** to change the port setting for spanning-tree. The following fields are available:

Instance ID (MSTP Only): a spanning-tree instance, you can configure MSTP on your switch to map multiple VLANs into a single STP instance.

Priority: sets the port priority in the switch. Low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 255.

Path Cost: the valid value is from 1 to 65535. Higher cost paths are more likely to be blocked by STP if a network loop is detected.

Link Type: By default, the link type is determined from the duplex mode of the interface: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection.

Edge Port: An edge port is the same as a Port Fast-enabled port, and you should enable it only on ports that connect to a single end station.

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To eventually make all changes permanent in Flash memory, go to **"Save Configuration" page** (bottom of management menu) and click **"Save"**.

Spanning tree – Port Parameters

7.7.2 Link Aggregation Static

This page configures the link aggregation static group (port trunking).

Port Selection Criterion: the algorithm to distribute packets among the ports of the link aggregation group according to source MAC address, destination MAC address, source and destination MAC address, source IP address, destination IP address, or source and destination IP address.

Trunk ID: a number to identify the trunk group besides the group name

Port: these port icons are listed the same way as on the front panel. You have to click on the icon to select the group members. The port can be removed from the group by clicking the selected port again.

Click **New** to create a new entry (temporary until **Submit** is clicked).

Click **Modify** to change settings of an existing entry (temporary until **Submit** is clicked).

Click **Remove** to remove an existing entry (temporary until **Submit** is clicked).

Click **Attach All** to select all ports for a selected entry (temporary until **Submit** is clicked).

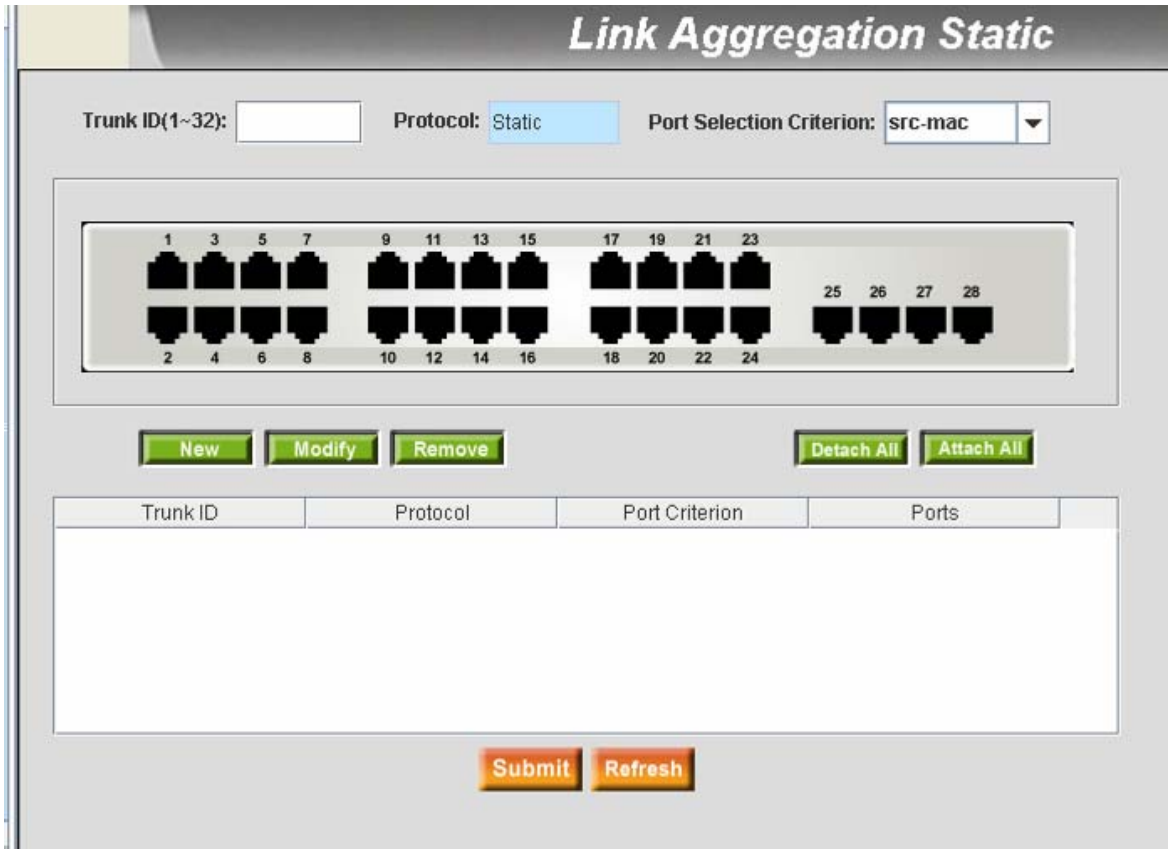
Click **Detach All** to unselect all ports for a selected entry (temporary until **Submit** is clicked).

Click **Submit** to set the changes to the connected Switch. Click **Refresh** to show the values of the Switch.

To eventually store all settings permanent in Flash memory, go to **"Save Configuration" page** (bottom of management menu) and click **"Save"**.

The user must check the runtime link speed and duplex mode to make sure the trunk is physically active. Go to Physical Interface and check the link mode in the runtime status window for the trunk ports. If all the trunk members are in the same speed and full duplex mode, then the trunk group is set up successfully. If one of the members is not in the same speed or full duplex mode, the trunk is not set correctly. Check the link partner and change the settings to have the same speed and full duplex mode for all the members of the trunk group.

- All the ports in the link aggregation group MUST operate in full-duplex mode at the same speed.
- All the ports in the link aggregation group MUST be configured in auto-negotiation mode or full duplex mode. This configuration will make the full duplex link possible. If you set the ports in full duplex force mode, then the link partner MUST have the same setting. Otherwise link aggregation could operate abnormally.
- All the ports in the link aggregation group MUST have the same VLAN setting.
- All the ports in the link aggregation group are treated as a single logical link. That is, if any member changes an attribute, the others will change also. For example, a trunk group consists of port 1 and 2. If the VLAN of port 1 changes, the VLAN of port 2 also changes with port 1.



Link Aggregation Static

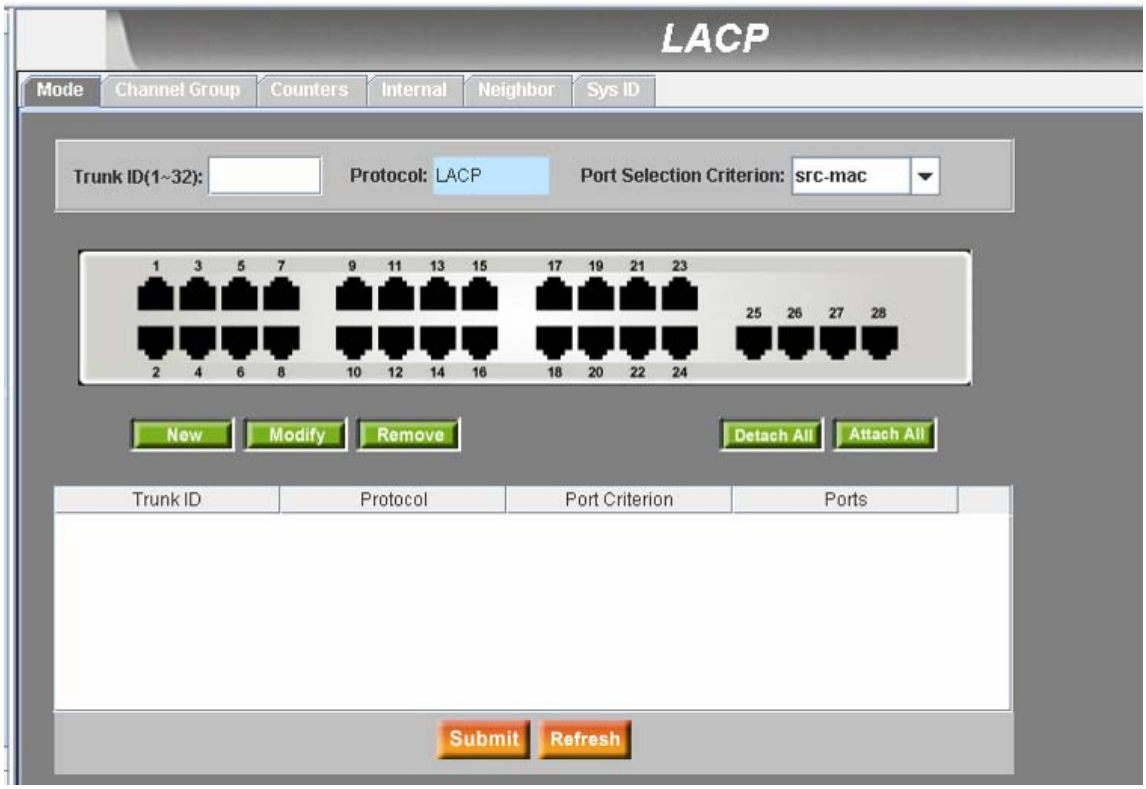
7.7.3 LACP

The page configures the LACP group (port trunking). The switch provides a maximum of 8 ports per group. For a standalone Switch, the maximum number of groups is 14 since it supplies 28 ports only. The feature supplies five statistics for verification.

Port Selection Criterion: the algorithm to distribute packets among the ports of the link aggregation group according to source MAC address, destination MAC address, source and destination MAC address, source IP address, destination IP address, or source and destination IP address.

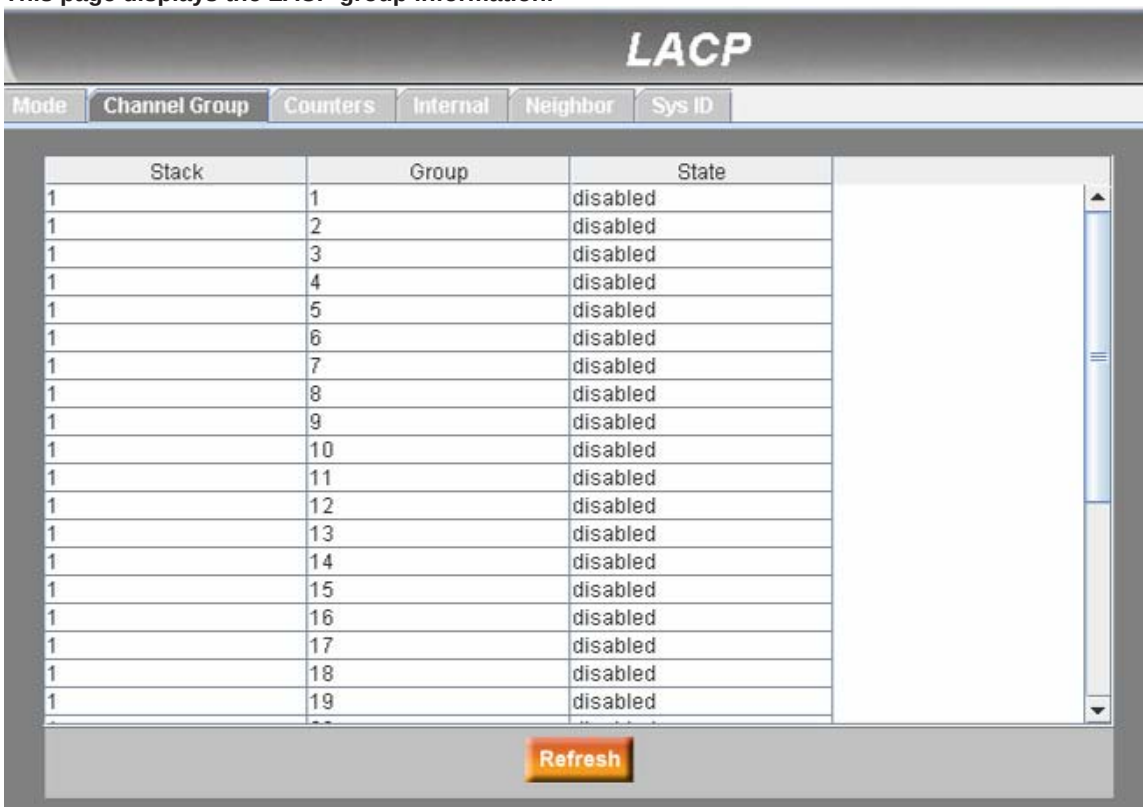
Trunk ID: a number to identify the trunk group besides the group name

Port: these port icons are listed the same way as on the front panel. The user should click on the icon to select the group members. The port can be removed from the group by clicking the selected port again.



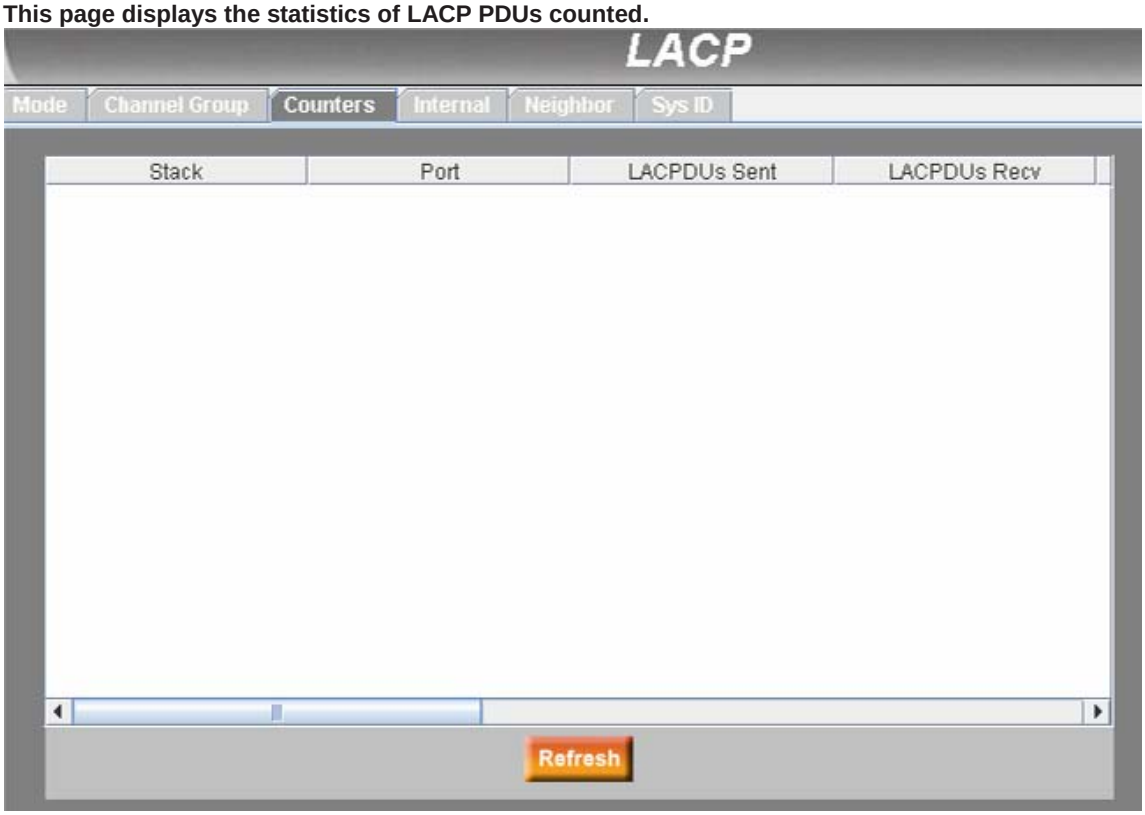
LACP – Mode

This page displays the LACP group information.



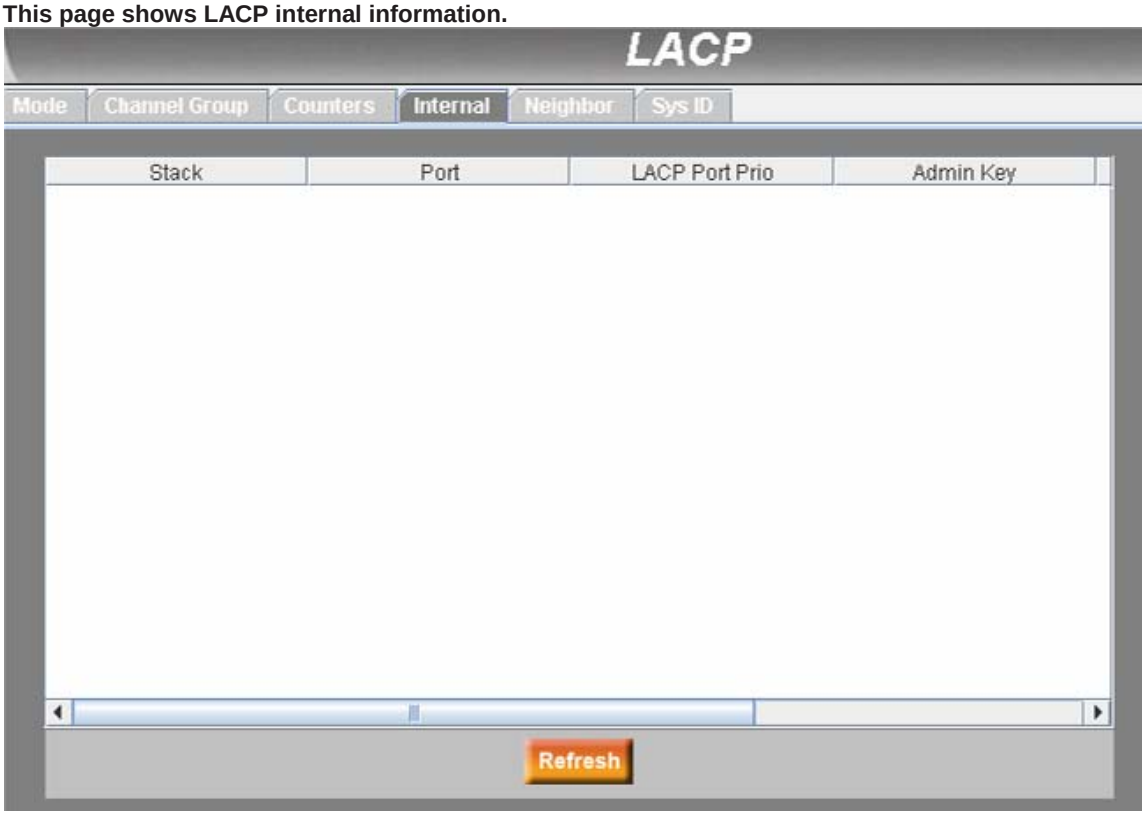
LACP – Channel Group

This page displays the statistics of LACP PDUs counted.



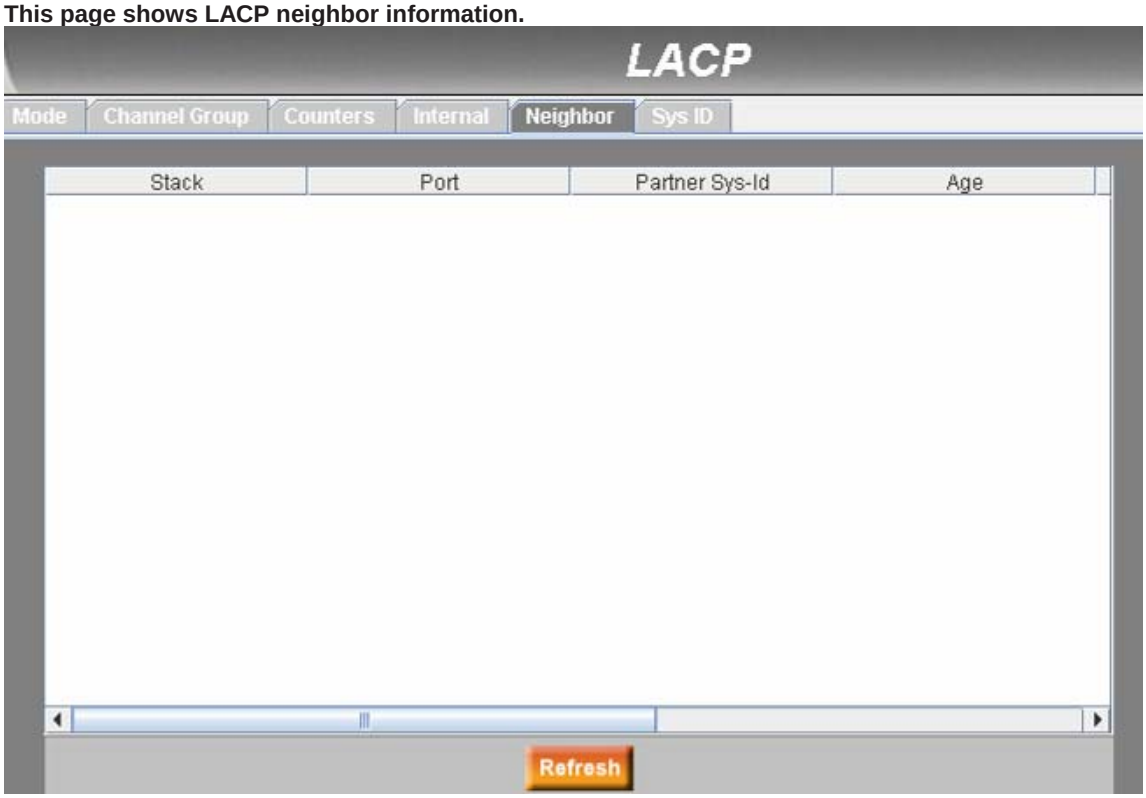
LACP – Counters

This page shows LACP internal information.



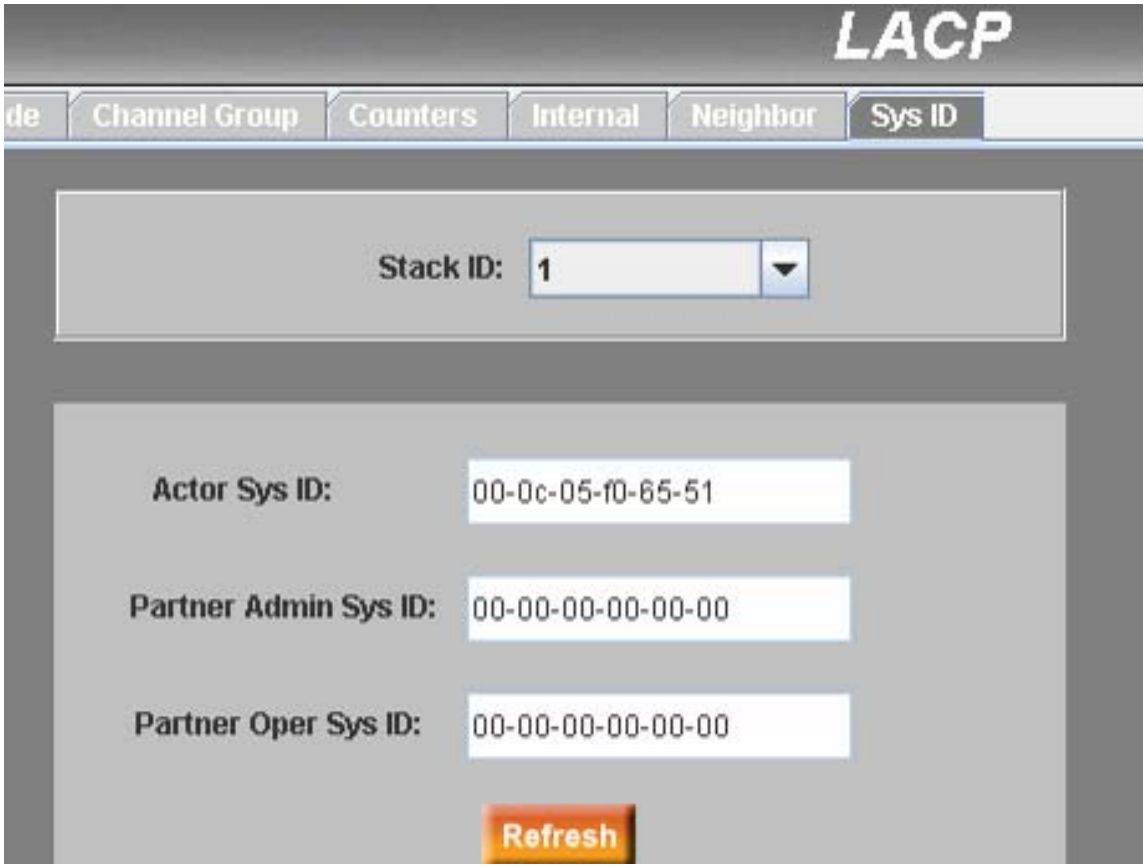
LACP – Internal

This page shows LACP neighbor information.



LACP – Neighbor

This page shows LACP system identification.



LACP – System ID

7.7.4 Mirroring

Port Mirroring, together with a network traffic analyzer, helps you monitor network traffics. You can monitor the selected ports for egress or ingress packets.

Mirror: Selects the mirrored port from selection panel. The selected port can be mirrored for Ingress, Egress or Both of traffic.

Mirror Mode: Enables or disables the mirror function for the selected group.

Stack ID: For a standalone switch, only ID 1 is available.

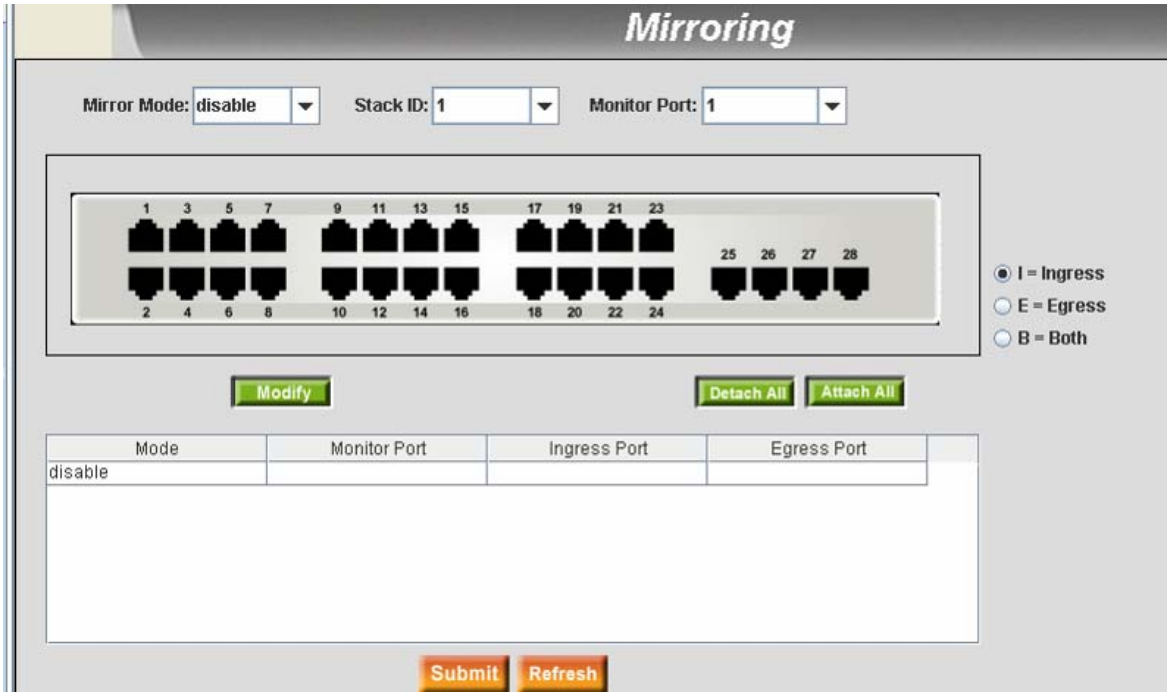
Monitor Port: Receives the copies of all the packets in the selected mirrored ports.

The monitor port cannot belong to any link aggregation group.

The monitor port cannot operate as a normal switch port. It does not switch packets or learn addresses.

Click **Submit** to set the changes to the connected Switch. Click **Refresh** to show the values of the Switch.

To eventually store all settings permanent in Flash memory, go to **"Save Configuration" page** (bottom of management menu) and click **"Save"**.



Mirroring

7.7.5 Static Multicast

This page can add multicast addresses into the multicast table. The switch can hold up to 256 multicast entries. All the ports in the group will forward the specified multicast packets to other ports in the group.

Port: selects the port from selection panel. Or select an existing group address from list panel to display

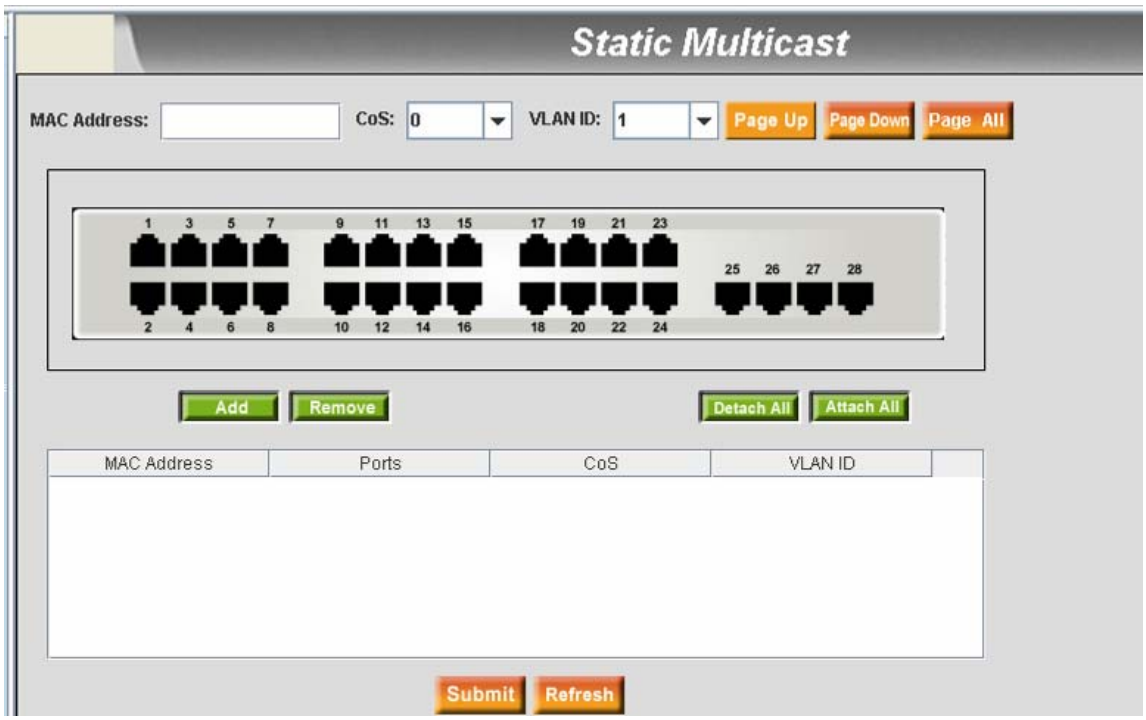
VLAN: selects the VLAN group, it is a VLAN-based feature

MAC Address: assigns the multicast address

CoS: assigns the priority for "Class of Service" of VLAN frames

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To eventually make all changes permanent in Flash memory, go to **"Save Configuration" page** (bottom of management menu) and click **"Save"**.



Static Multicast

7.7.6 IGMP Snooping

IGMP Snooping helps reduce the multicast traffic on the network by allowing the IGMP snooping function to be turned on or off.

The first part provides the following settings,

Enable IGMP Snooping: Globally enable IGMP snooping in all existing VLAN interfaces. By default, IGMP snooping is globally disabled on the switch. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces.

If global snooping is disabled, the user cannot enable VLAN snooping. If global snooping is enabled, the user can enable or disable VLAN snooping.

Last Member Query Interval: Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership.

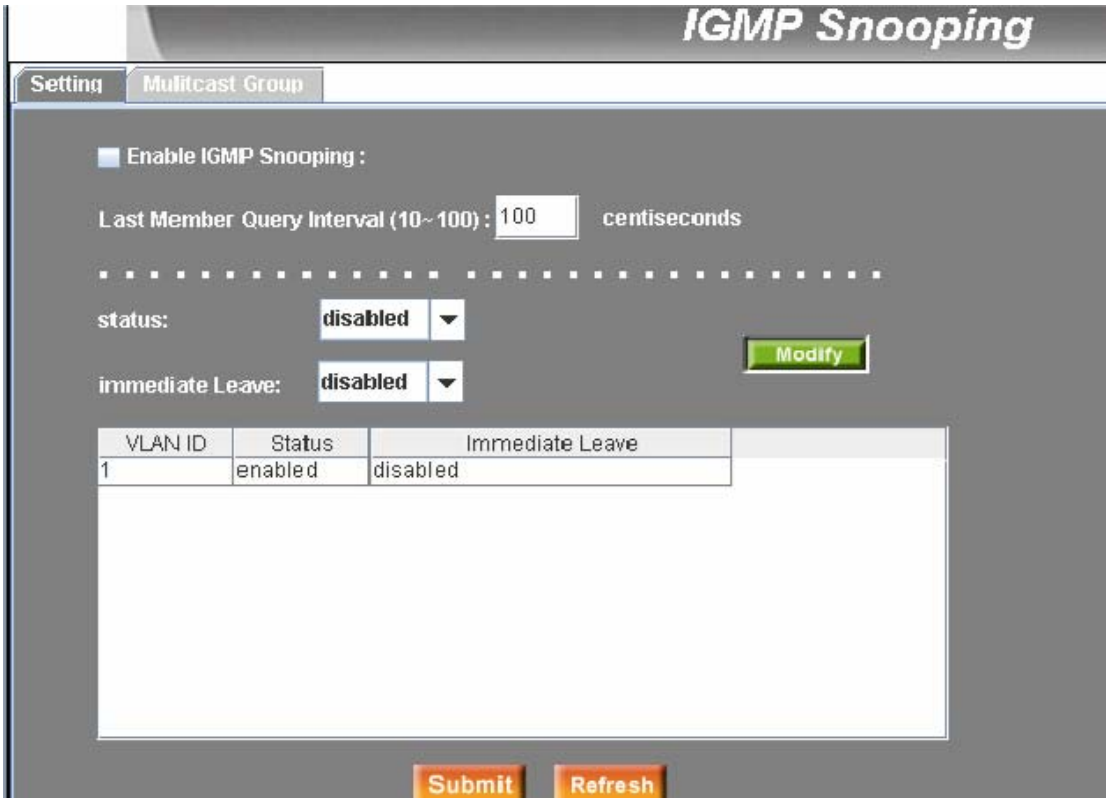
The second part provides the following settings:

Status: If global snooping is enabled, the user can enable or disable VLAN snooping.

Immediate leave: When the user enables IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. The user should use the Immediate Leave feature only when there is a single host present on every port in the VLAN. Immediate Leave is supported with only IGMP version 2 hosts.

If the static entries occupy all 256 spaces, IGMP snooping does not work normally.

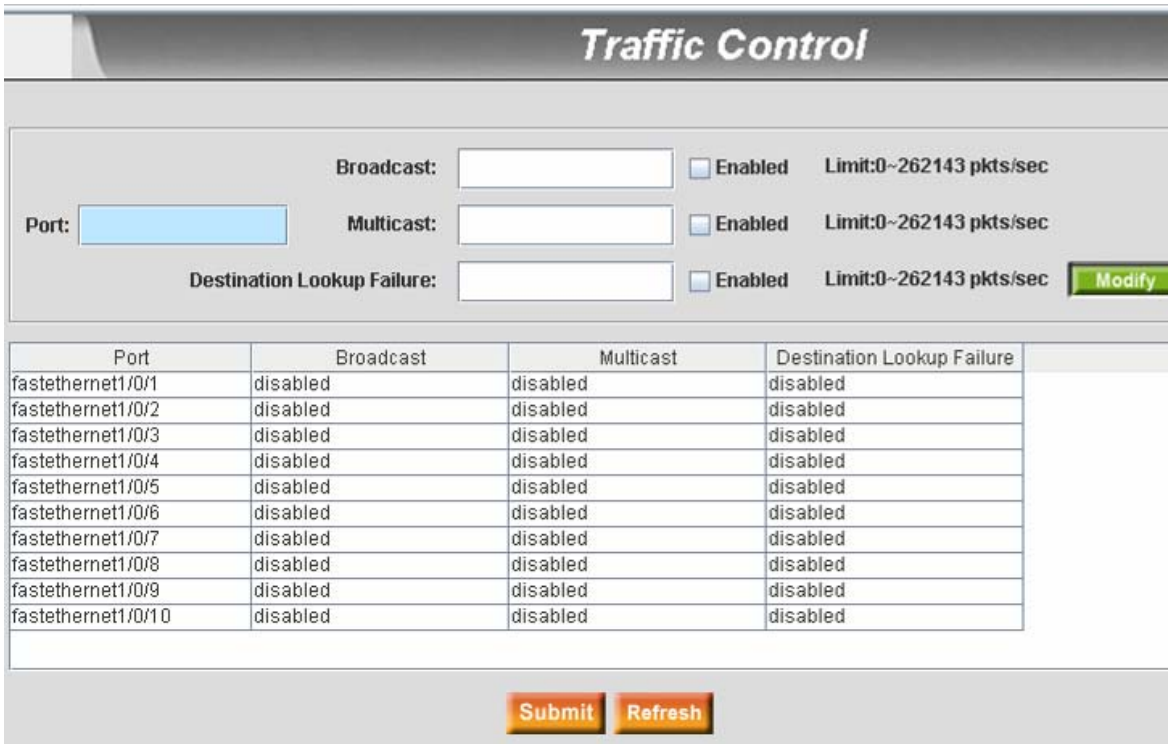
The Switch only allows 256 Layer 2 multicast groups.



IGMP Snooping – Setting

IGMP Snooping – Multicast Group

7.7.7 Traffic Control



Traffic Control

Traffic Control protects the Switch bandwidth from flooding packets – including broadcast packets, multicast packets and unicast packets – caused by destination address lookup failure. The limit number is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value.

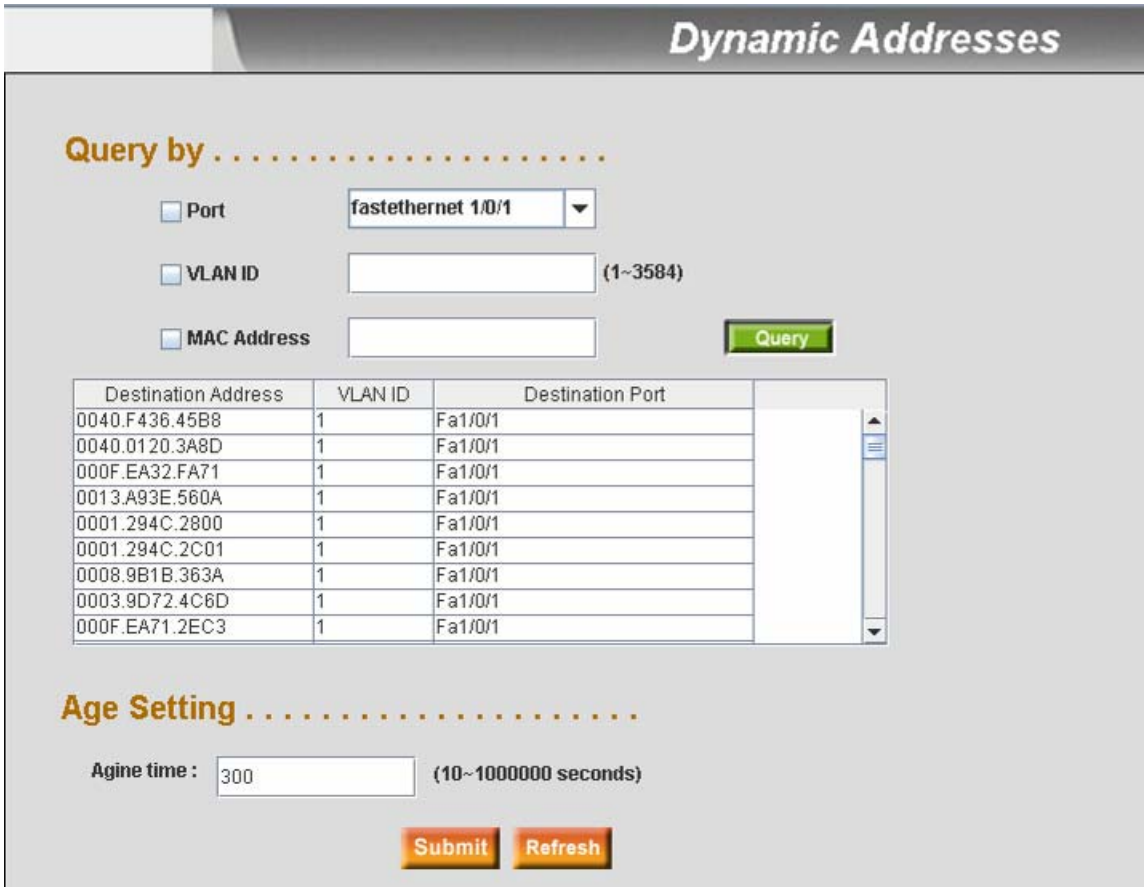
Select an interface and assign the desirable settings, then click **Modify**.

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To eventually make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.

7.7.8 Dynamic Addresses

This page displays the results of dynamic MAC address look-up by port, VLAN ID, or specified MAC address. The dynamic address is the MAC address learned by the Switch. It will age out of the address table if the address is not learned again within the aging time limit. The user can set the aging time by entering 10 to 1,000,000 in seconds. Click on **Submit** to save the new values. **Refresh** will show the effects of the setting changes. The user can look up MAC addresses by checking and filling the options for port, VLAN ID, or/and MAC address, then click **Query**. The address window will display the results of the query.



Dynamic Addresses

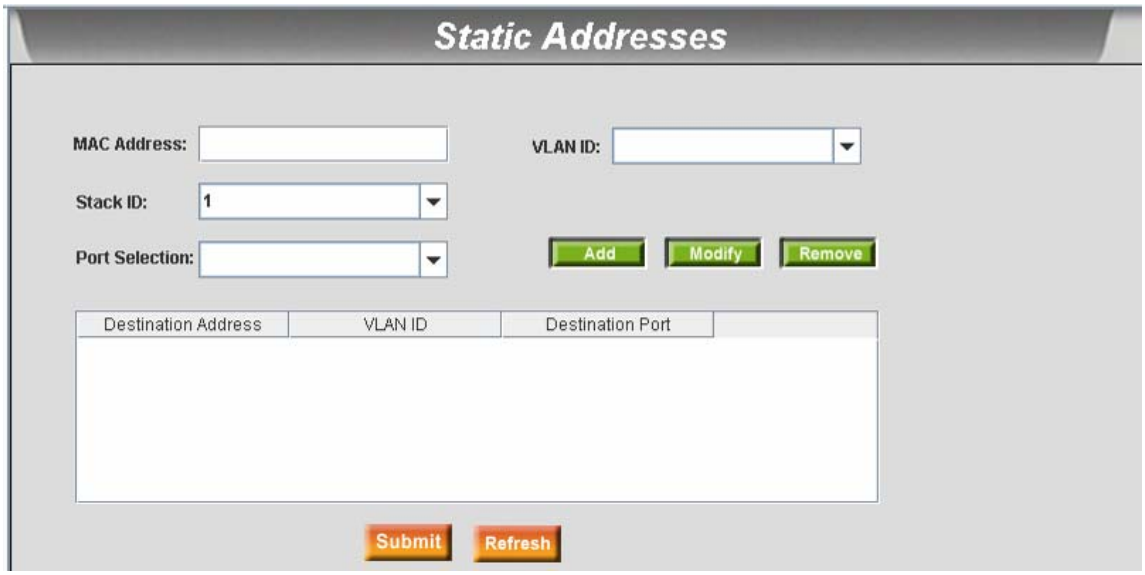
7.7.9 Static Addresses

The user can add a MAC address to the switch address table. The MAC address added in this way will not age out from the address table. These are called static addresses.

MAC Address: enter the MAC address
VLAN ID: enter the VLAN ID that the MAC belongs to
Stack ID: For a standalone switch, only ID 1 is available
Port Selection: select the port which the MAC belongs to

Click **Add** to create a new static MAC address with the above information (temporary until **Submit** is clicked). Click **Remove** to remove a selected entry (temporary until **Submit** is clicked). Click **Modify** to update an existing MAC address entry (temporary until **Submit** is clicked).

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes. To eventually make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.



Static Addresses

7.7.10 VLAN Configuration

The user can create up to 4094 VLAN groups and show the VLAN groups in this page. VLAN1 is the default VLAN, which is created by the system. It cannot be removed. This feature prevents the switch from malfunctioning. You can remove any existing VLAN except VLAN1.

The user can assign the port to be a tagged port or an untagged port by clicking on the port on the picture. There are three types of buttons in the port selection panel:

"U" type: An untagging port that will remove VLAN tags from the transmitted packets.

"T" type: All packets transmitted from this port will be tagged.

If the port is left "blank": This port is not a member of the selected VLAN group.

If one untagging port belongs to two or more VLAN groups at the same time, it will confuse the switch and cause flooding traffic. To prevent this, the switch only allows one untagging port to belong to one VLAN at the same time.

If the user wants to assign an untagging port from one VLAN to another, you first have to change it into something else in the original VLAN.

VLAN ID: requires the user to enter the VLAN ID when a new VLAN is created

Name: requires the user to assign a name for the VLAN

DHCP-Snooping : requires the user to assign a name for the VLAN

Click **New** to create a new entry (temporary until **Submit** is clicked).

Click **Add** to add new entry to list of entries (temporary until **Submit** is clicked).

Click **Modify** to temporarily save changes to an existing entry (temporary until **Submit** is clicked).

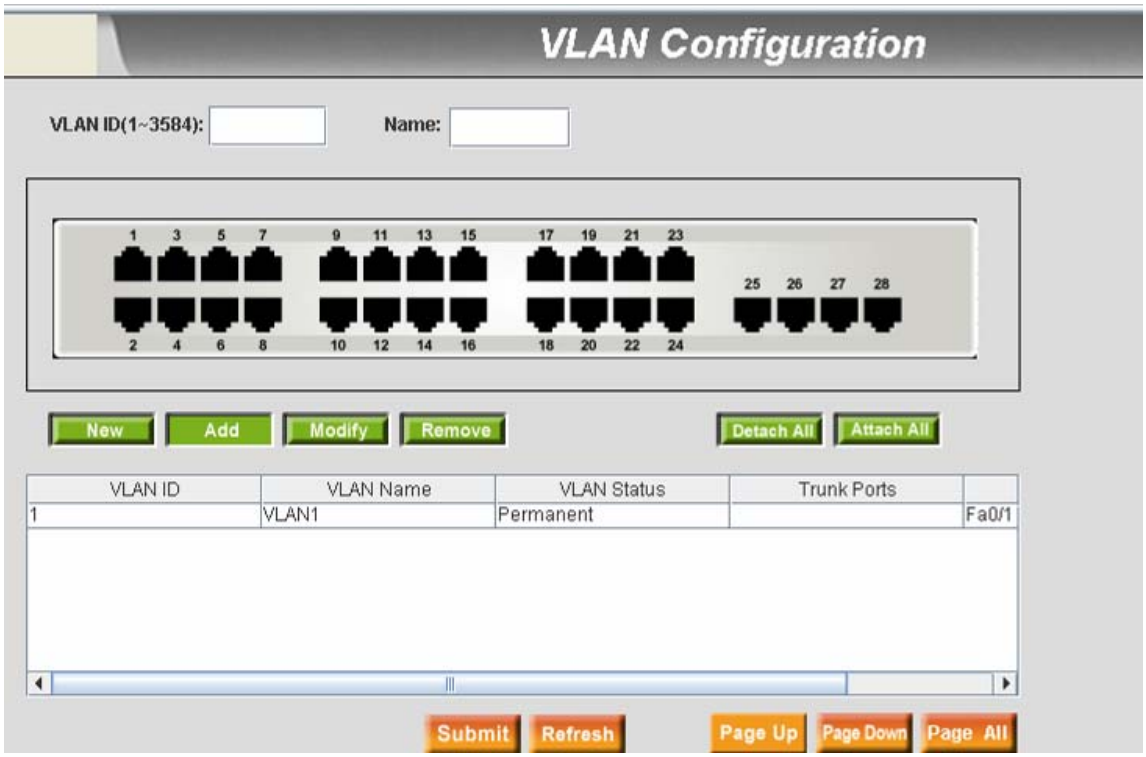
Click **Remove** to remove selected entry (temporary until **Submit** is clicked).

Click **Attach All** to select all ports for a selected entry (temporary until **Submit** is clicked).

Click **Detach All** to unselect all ports for a selected entry (temporary until **Submit** is clicked).

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all changes permanent in Flash memory, go to **"Save Configuration" page** (bottom of management menu) and click **"Save"**.



VLAN Configuration

7.7.11 GVRP

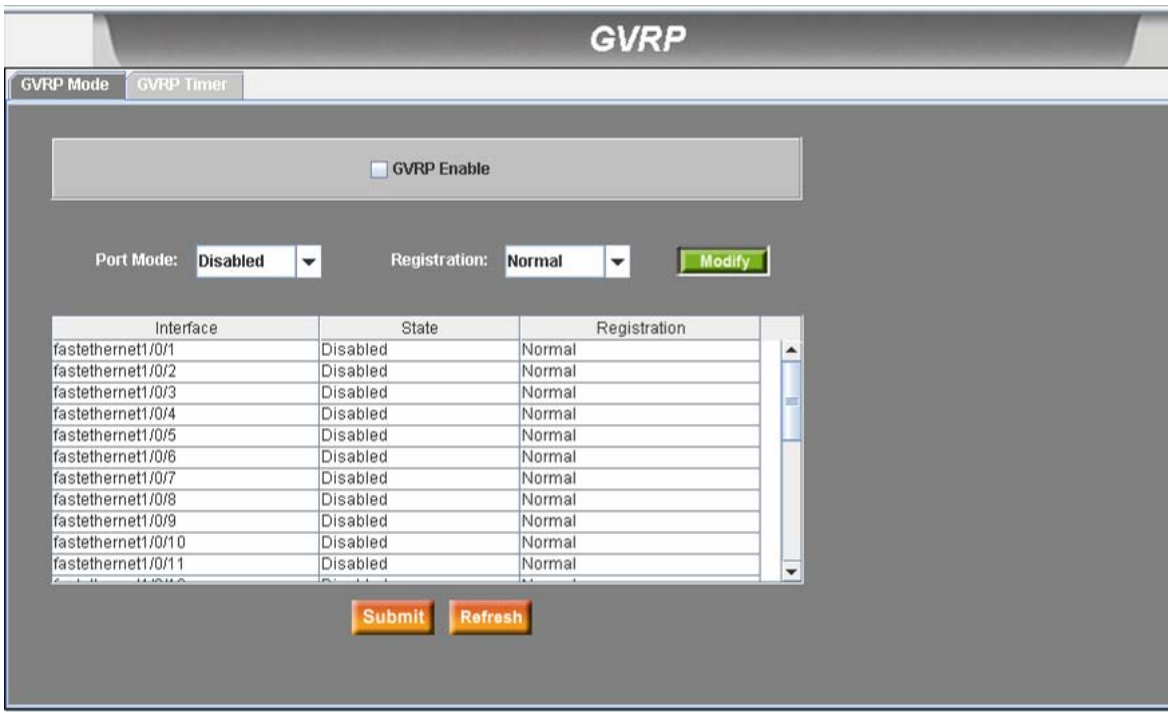
Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) is an application defined in the IEEE 802.1Q standard that allows for the control of VLANs.

GVRP will run only on 802.1Q trunk ports and is used primarily to prune traffic from VLANs that does not need to be passed between trunking switches. There are some parameters to configure GVRP:

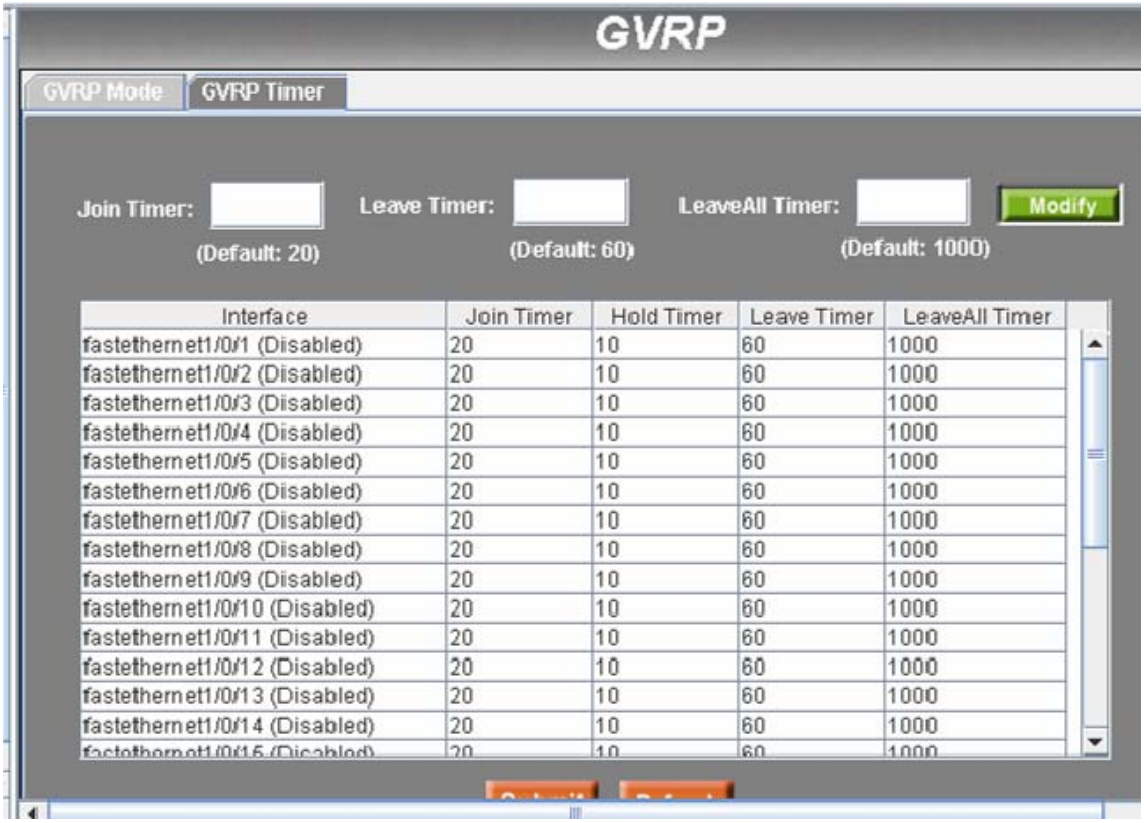
GVRP Enable: By default GVRP is not enabled for the switch. You must first enable GVRP on the switch before you can configure the 802.1Q ports for GVRP operation.

Port Mode: enables/disables GVRP on the individual 802.1Q trunk port. GVRP must be configured on both sides of the trunk to work correctly.

Registration: By default GVRP ports are in normal registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the fixed mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in forbidden mode forward only for VLAN 1.



GVRP – GVRP Mode



GVRP – GVRP Timer

7.7.12 QoS/CoS

7.7.12.1 802.1p Priority

Each port has eight egress queues. These queues can either be configured with the Weighted Round Robin (WRR) scheduling algorithm or with one queue as a strict priority queue and the other queues for WRR. The strict priority queue must be empty before the other queues are serviced. You can use the strict priority queue for mission-critical and time-sensitive traffic. There are three options:

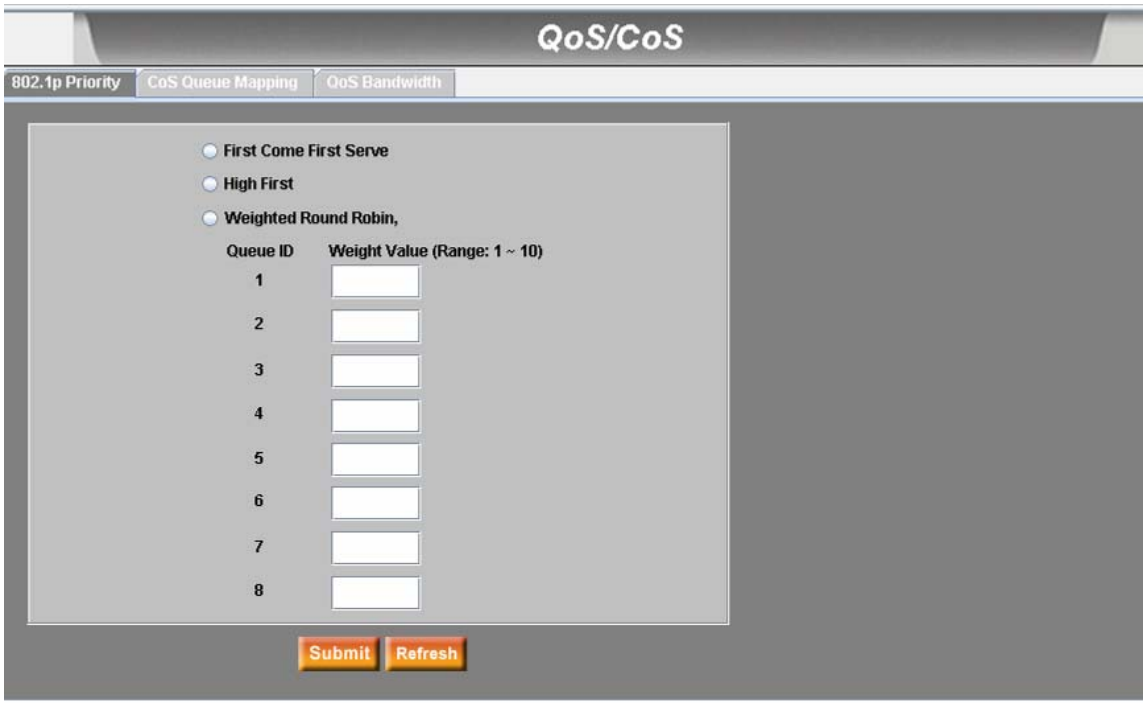
First Come First Service: the first come frame has the highest priority

High First: Packet's priority depends on its CoS value

Weighted Round Robin (WRR): If WRR scheduling algorithm is enabled, the ratio of the weights is the ratio of frequency in which the WRR scheduler de-queues packets from each queue.

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.



QoS/CoS – 802.1q Priority

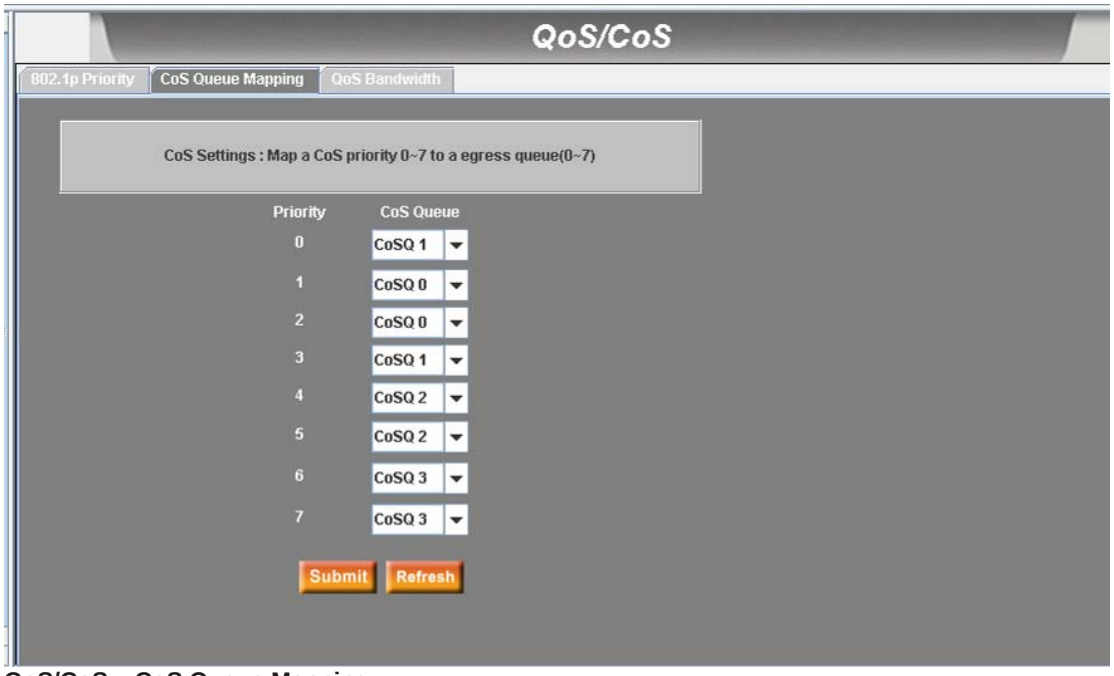
7.7.12.2 QoS Queue Mapping

The switch supports eight egress queues for each port with a strict priority scheduler. That is, each CoS value can map into one of the eight queues. Queue eight has the highest priority to transmit packets.

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.

The CoS values range from 0 for low priority to 7 for high priority.



QoS/CoS – CoS Queue Mapping

7.7.12.3 QoS Bandwidth

Some VLAN tag-related field settings for each port are included in this page. It includes:

Port: Select a port from list window to configure

Ingress Bandwidth: Maximum ingress bandwidth in 64kbps steps for selected port

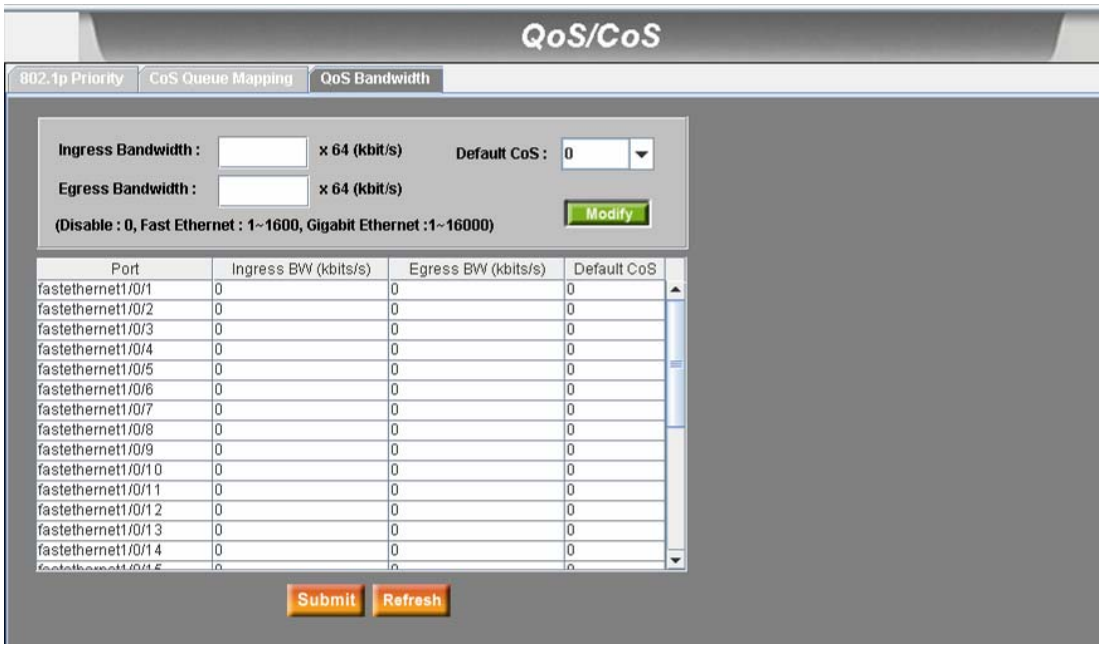
Egress Bandwidth: Maximum egress bandwidth in 64kbps steps for selected port

Default CoS: every untagged packet received from this port will be assigned to this CoS value in the VLAN tagged

Click on **Modify** to change the content in the selected port's window (temporary until **Submit** is clicked).

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.



QoS/CoS – QoS Bandwidth

7.8 SNMP

This group offers the SNMP configuration including Host Table and Trap Setting

7.8.1 Host Table

This page links host IP address to the community name that is entered in Community Table page. Type an IP address and select the community name from the drop-down list.

Click **Add** to add new entry to list of entries (temporary until **Submit** is clicked).

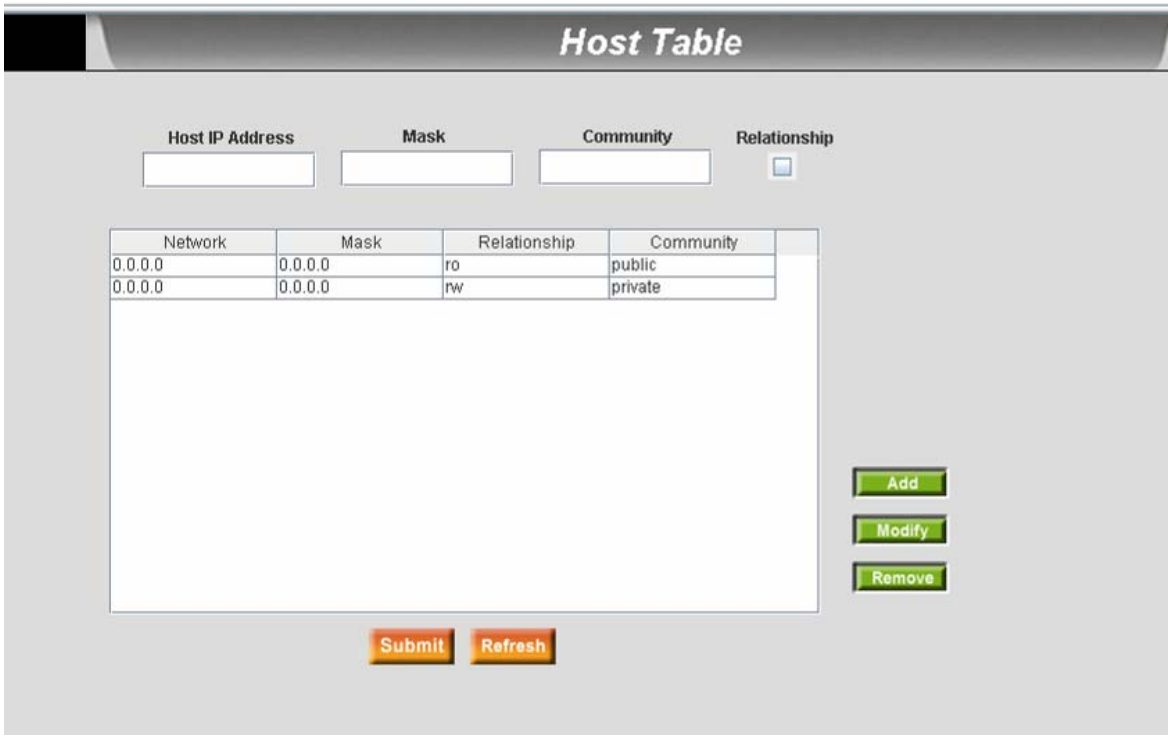
Click **Modify** to temporarily save changes to an existing entry (temporary until **Submit** is clicked).

Click **Remove** to remove selected entry (temporary until **Submit** is clicked).

Check Relationship for creating Set Community name, and uncheck Relationship for creating Get Community name.

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.



Host Table

7.8.2 Trap Setting

By setting trap destination IP addresses and community names, you can enable SNMP trap function to send trap packets in different versions (v1 or v2c).

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.

Trap Setting

7.8.3 SNMPv3 VGU Table

Two concepts represent the new security features defined by SNMPv3:

1) The User-based Security Model (USM), which provides authentication, encryption, and decryption of SNMPv3 packets.

2) The View-based Access Control Model (VACM), which provides access control.

The following three pages are related:

Click **Add** to add new entry to list of entries (temporary until **Submit** is clicked).

Click **Modify** to temporarily save changes to an existing entry (temporary until **Submit** is clicked).

Click **Remove** to remove selected entry (temporary until **Submit** is clicked).

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.

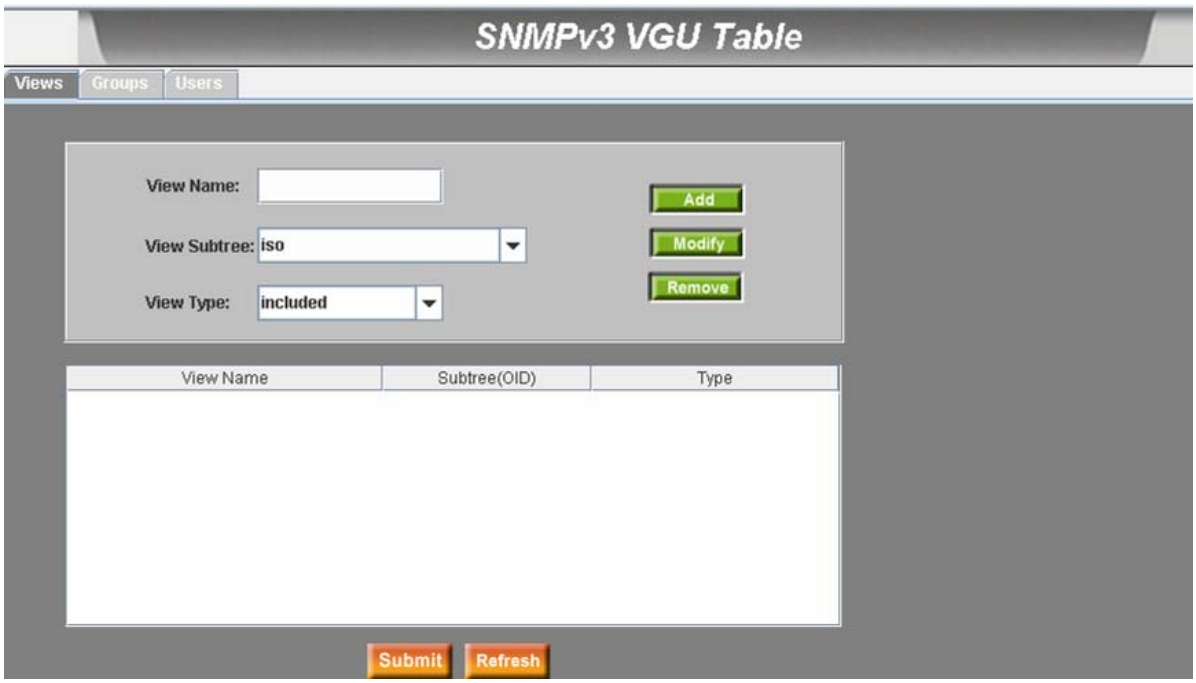
7.8.3.1 View

VACM View is used to view the information of SNMPV3 VACM Group.

View Name: enter the security group name.

View Type: enter the View Type that the View belongs to. Included or Excluded when View Subtree matches the Oid in the SNMPv3 message.

View Subtree: enter the View Subtree that the View belongs to. The Subtree is the Oid to match the Oid in the SNMPv3 message. The match is good when the subtree is shorter than the Oid in the SNMPv3 message.



SNMPv3 VGU Table – Views

7.8.3.2 Groups

VACM Group is used to configure the information of SNMPV3 VACM Group.

Group Name: enter the security group name.

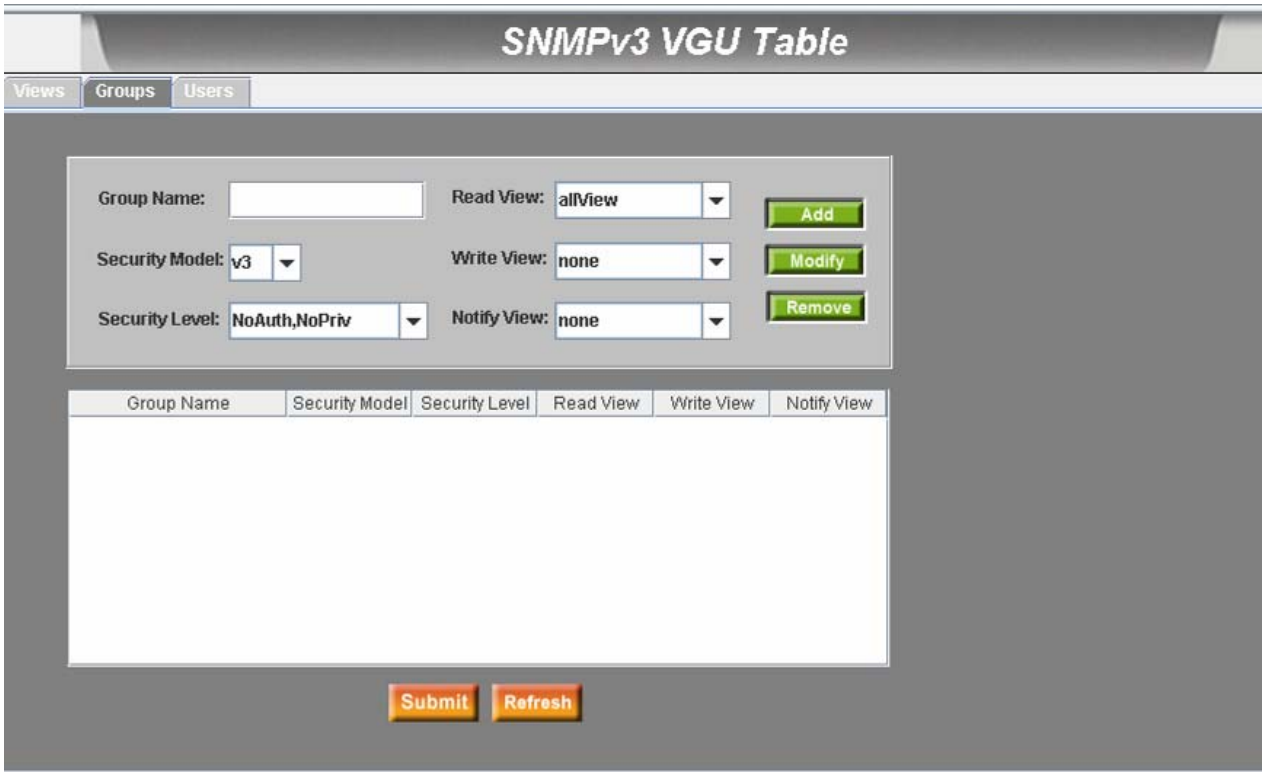
Read View Name: enter the Read View Name that the Group belongs to. The related SNMP messages are Get, GetNext, GetBulk.

Write View Name: enter the Write View Name that the Group belongs to. The related SNMP message is Set.

Notify View Name: enter the Notify View Name that the Group belongs to. The related SNMP messages are Trap, Report.

Security Model: enter the Security Model Name that the Group belongs to. Any is suitable for v1,v2,v3. USM is SNMPv3 related.

Security level: enter the Security level Name that the Group belongs to. Only NoAuth, AuthNopriv, AuthPriv can be chosen.



SNMPv3 VGU Table – Groups

7.8.3.3 Users

USM User is used to configure the information of SNMPV3 USM User.

User Name: User name of a specific security group

Group Name: enter the security group name

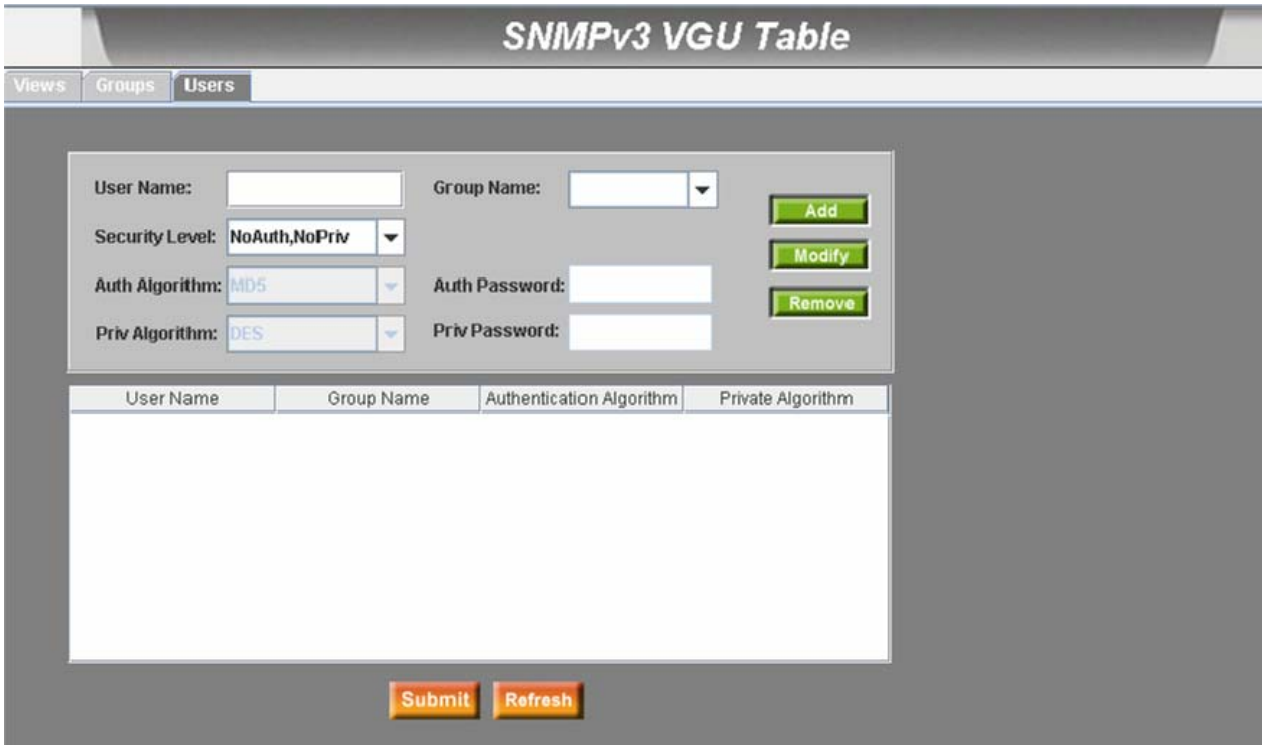
Auth Protocol: enter the Auth Protocol that SNMP User and Security Group belong. Only NoAuth ,MD5, SHA1 can be chosen. If the NoAuth is chosen, there is no need to enter password.

Auth Password: enter the password that the Auth Protocol belongs. The password needs at least 8 characters or digits.

Priv Protocol: enter the Priv Protocol that SNMP User and Security Group belong. Only NoPriv, DES can be chosen. If the NoPriv is chosen, there is no need to enter password.

Priv Password: enter the password that the Priv Protocol belongs. The password needs at least 8 characters or digits.

Security level: enter the Security level Name that the Group belongs. Only NoAuth, AuthNopriv, AuthPriv can be chosen.



SNMPv3 VGU Table – Users

7.9 ACL

The switch can set Access Control List rules to filter certain traffic types according to packet header information from Layer 2 to Layer 4. Each filter set includes a couple of rules. The user should attach the filter set to certain ports to make the filter work.

7.9.1 Set Access Control List

The Switch defines two modes of rules, one is MAC mode and the other is IP mode. Only the same mode of rules can bundle together to form a filter set. Each mode has different fields to configure. For example, the user can use the IP mode rule to filter FTP packets.

The user can check the MAC Filter, give it a Name then add it. The user also can check the IP Filter and give it an ID/Name, then click on **Add**. Click **Submit** to save the configuration permanently or **Refresh** to refresh the page. Please click **Edit** before

editing.

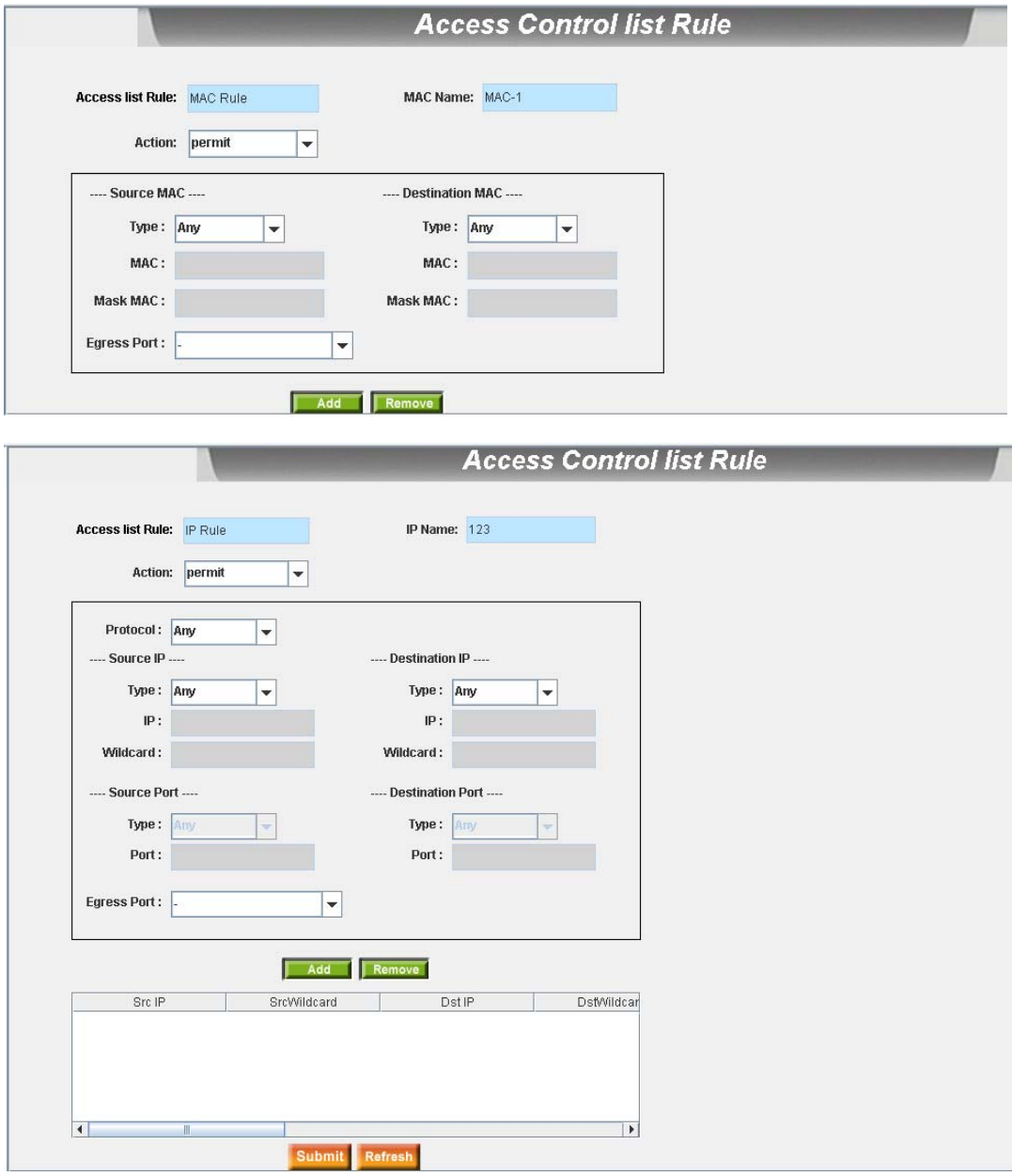
Click on a filter set to select the set to be edited or removed. Second, click on **Edit** to enter the rule page, or click on **Remove** to remove the filter set. The user should follow the rules to make a valid filter set.

One set consists of a collection of rules. The rules having the same fields to filter packets belong to one type. For example, two rules which filter packets with two destination IP addresses, belong to the same type. But a rule filtering source IP address does not belong to the same type.

Four types of rules can apply to ports at the same time. If there are more than four types, the system automatically disables the rules.

Set ACL

The Filter Rule page provides attributes of rule modes; one is for MAC rule and the other is for IP rule. If the user did not enter a MAC address in the blank box, the rule set will pay no attention to the MAC value. In an IP rule setup, you can enter any of the 5 types: source IP, destination IP, protocol, source application port and destination application port. The Action field determines if the packet should be dropped or forwarded when it matches the rule. If a packet matches two rules with different consequences, the packet will follow the rule which appears first in the rule list.



Access Control List Rule

7.9.2 Apply Access Control List

An ACL rule is idle if it is not attached to any ingress port. Use the Apply Access Control List page to attach a filter set to ingress ports.

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to **Save Configuration page** (bottom of management menu) and click **Save**.

To apply an ACL rule to ports:

Attach to all ports: the ACL rule applies to all the ports of the system.

Attach to certain ports: the ingress ports to be applied can be specified.

Detach from all ports: remove all the ACL rules from the attached ports.

NOTE: The user may not detach certain ports after issuing an "Attach All" command. To detach ports, use the "Detach All" command.

NOTE: Once the ACL rule is attached to the ingress ports, it will filter the packets according to the ingress port and the packet fields in the rules. For example, a set with a single rule to filter out destination MAC address 00:10:20:30:40:50 is attached to ingress port 3. A packet with destination MAC 00:10:20:30:40:50 from port 3 is not permitted.

Apply Access Control list
Access list ID/Name:
Detach All
Attach All
1 3 5 7 9 11 13 15 17 19 21 23
25 26 27 28
2 4 6 8 10 12 14 16 18 20 22 24
I = Ingress
Submit
Refresh

Apply Access Control List

7.9.3 Content Aware

A set of Content Aware rules can be set to process specified types of service packets, rather than taking efforts to identify layer-4 TCP or UDP connection types and their port numbers. The network administrator can choose to block those packets, or adjust the packet contents as high or low priority.

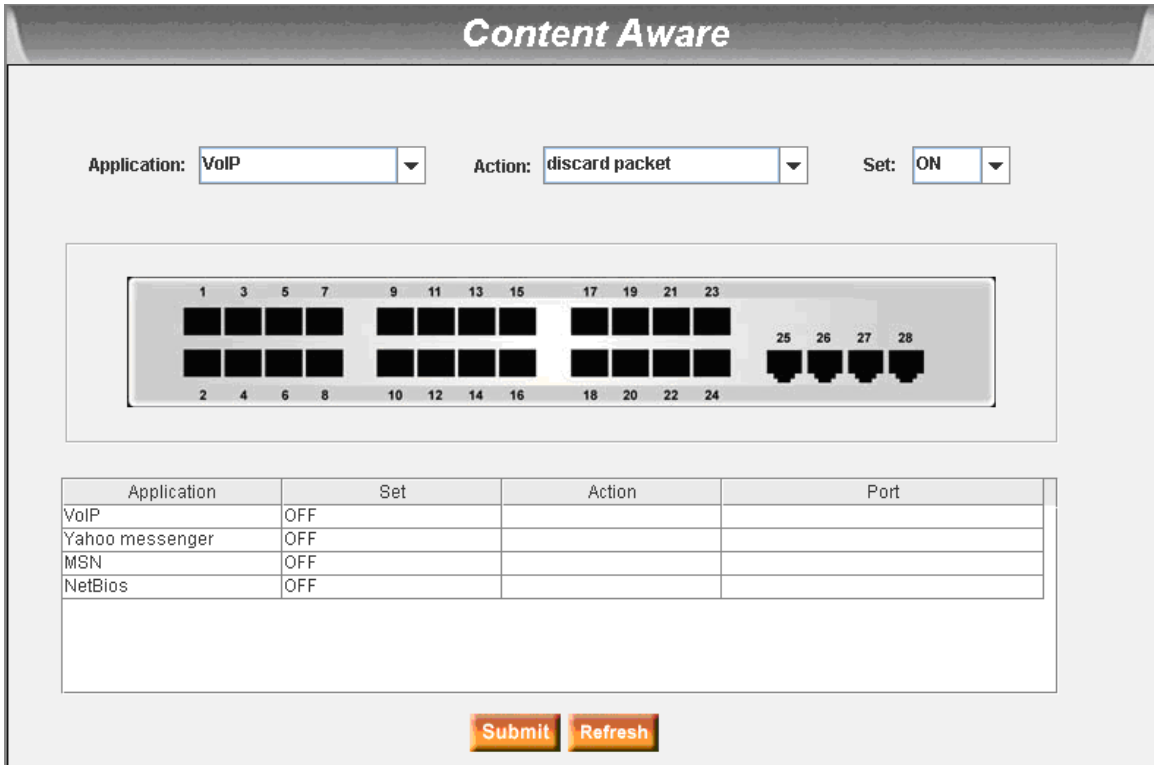
Packet Type: type of packets to be processed. Choose between VoIP, Yahoo Messenger, MSN, NetBios.

Action: the action to the chosen packets, including "discard packet", "Set 802.1P priority high (7)" (For VoIP only), and "Set 802.1P priority low (0)" (For VoIP only).

Set: "**ON**" to set the rule, and "**OFF**" to disable the rule.

Click the ports which the rules are applied to and click **Submit** to save changes on-line. Click **Refresh** to view effect of changes.

To eventually make all changes permanent, go to **Save Configuration page** (bottom of management menu) and click **Save**.



Content Aware

7.10 Security

The switch supports the 802.1x port-based security feature. Only authorized hosts are allowed to access the switch port. Traffic from unauthenticated hosts will be blocked. Authentication can be provided via a RADIUS server or the local database in the switch.

The switch also supports dynamic VLAN assignment through 802.1x authentication process. The VLAN information for the users/ports should be configured in the authentication server properly before enabling this feature.

7.10.1 Port Access Control

Port Access Control is used to configure various 802.1x parameters. 802.1x uses either RADIUS server or local database to authenticate port users.

The first part is the Bridge (Global) settings:

Sys-Auth-Control: checks it to enable the authentication

Authentication Method: RADIUS or Local database can be used to authenticate the port user.

The second part is the port settings:

Port: Specify which port to configure from port list window.

Multi-host: If enabled, ALL hosts connected to the selected port are allowed to use the port if ONE of the hosts passed the authentication. If disabled, only ONE host is allowed to use the port.

Authentication Control: If “ForceAuthorized” is selected, the selected port is forced authorized. Thus, traffic from all hosts is allowed to pass. Otherwise, if “ForceUnauthorized” is selected, the selected port is blocked and no traffic can go through. If “Auto” is selected, the behavior of the selected port is controlled by 802.1x protocol. All ports should be set to “Auto” under normal conditions.

Reauthentication: Once enabled, the switch will try to authenticate the port user again when the re-authentication time is up.

ReAuthentication Time: If “Reauthentication” is enabled, this is the time period the switch uses to re-send authentication request to the port user (see above).

Quiet Period: If authentication fails, the switch waits for this time period before sending another authentication request to the port user.

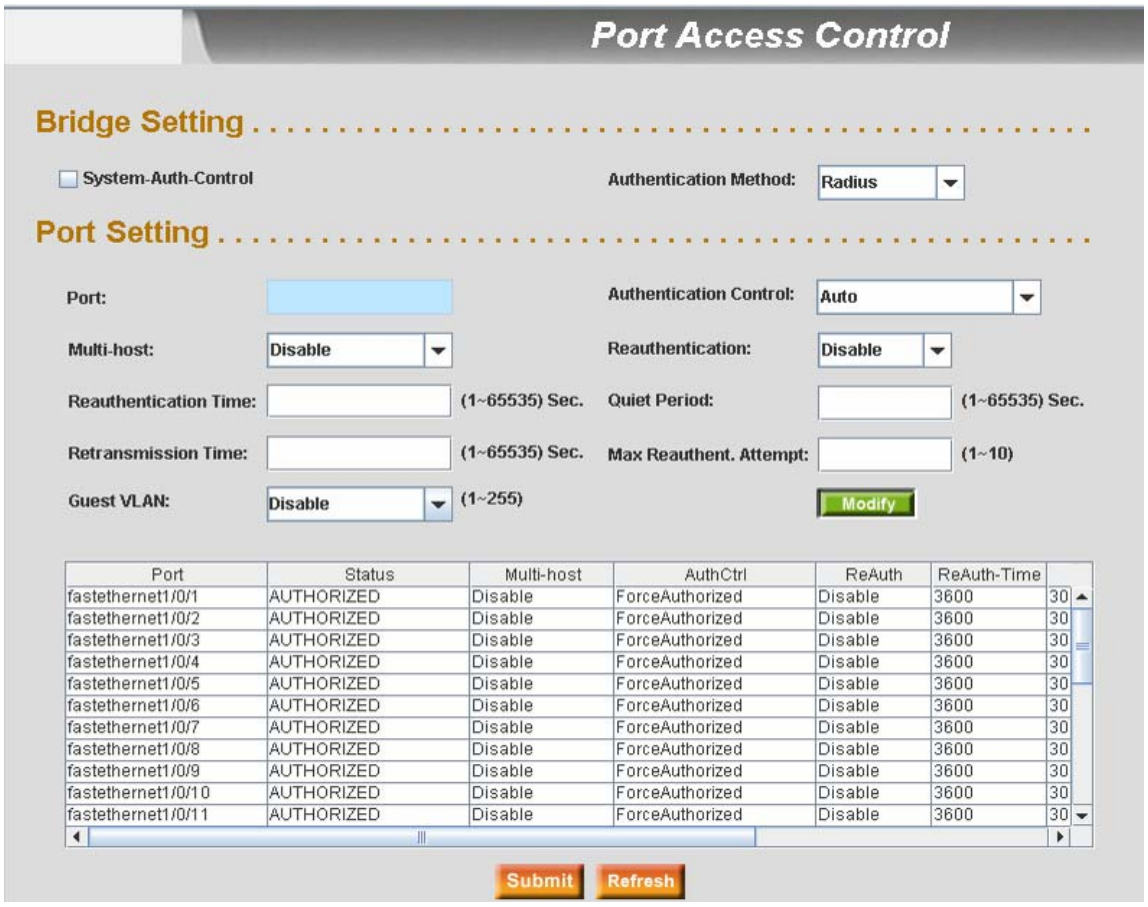
Retransmission Time: If the port user failed to respond to authentication request from the switch, the switch waits for this time period before sending another authentication request to the port user.

Max Reauthent Attempt: Retry count if the port user fails to respond to authentication requests from the switch.

Guest VLAN: Specify a guest VLAN for clients that are not 802.1x-capable.

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all the changes permanent in Flash memory, go to the **Save Configuration page** (bottom of management menu) and click **Save**.



Port Access Control

7.10.2 Dial-in User

Dial-in User is used to define users in the local database of the switch.

User Name: New user name.

Password: Password for the new user.

Confirm Password: Enter the password again.

VLAN ID: Specify the VLAN ID assigned to the 802.1x-authenticated clients.

Please click **Add** to add the new user. Click **Modify** when the modifications have been entered. Click **Remove** when you want to remove the selected user. Click **Submit** to make the settings permanent. Click **Refresh** to refresh the settings to current value.

Dial-in User

7.10.3 RADIUS

In order to use an external RADIUS server, the following parameters must be configured:

Authentication Server IP: The IP address of the RADIUS server.

Authentication Server Port: The port number that the RADIUS server is listening to.

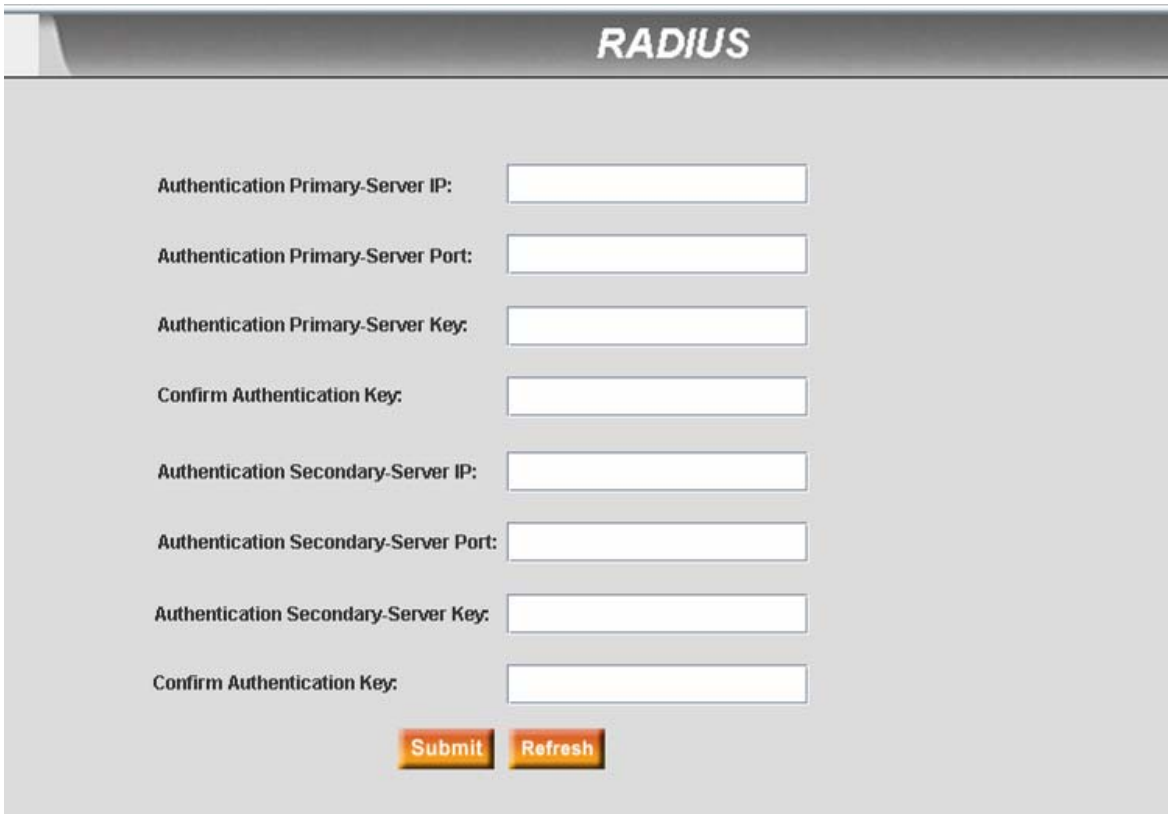
Authentication Server Key: The key that is used for communications between the Switch and the RADIUS server.

Confirm Authentication Key: Re-type the key entered above.

NOTE: The VLAN of the RADIUS server connected to the switch must be the same as the VLAN of the system management interface.

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To eventually make all the changes permanent in Flash memory, go to the **Save Configuration page** (bottom of management menu) and click **Save**.

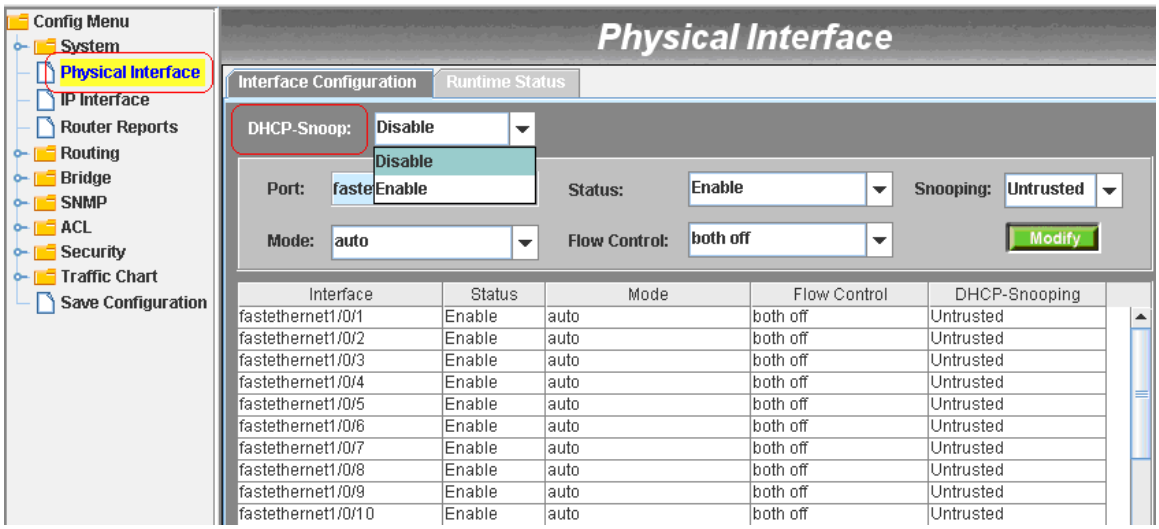


Radius

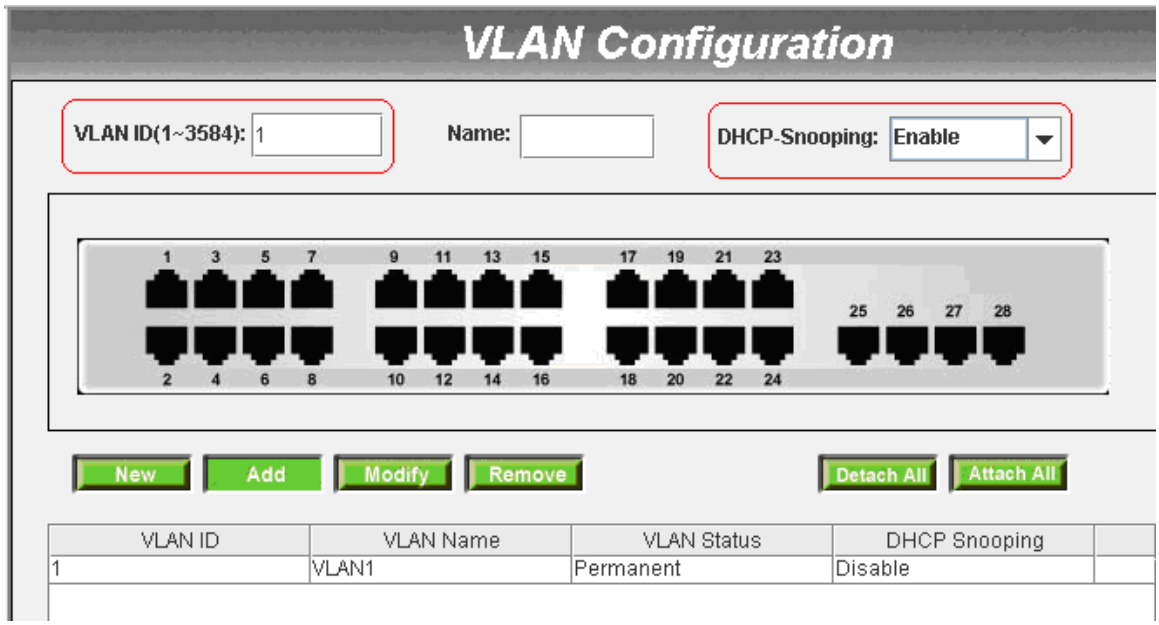
7.10.4 IP DHCP Snooping

In order to filter unwanted DHCP response, you can enable DHCP filtering function to allow DHCP response back from the special port(s) where real DHCP server stands.

To enable this function, go to physical interface configuration page, select ‘Enable’ at ‘DHCP-Snoop’ item, then click ‘summit’ to apply the global configuration setting.

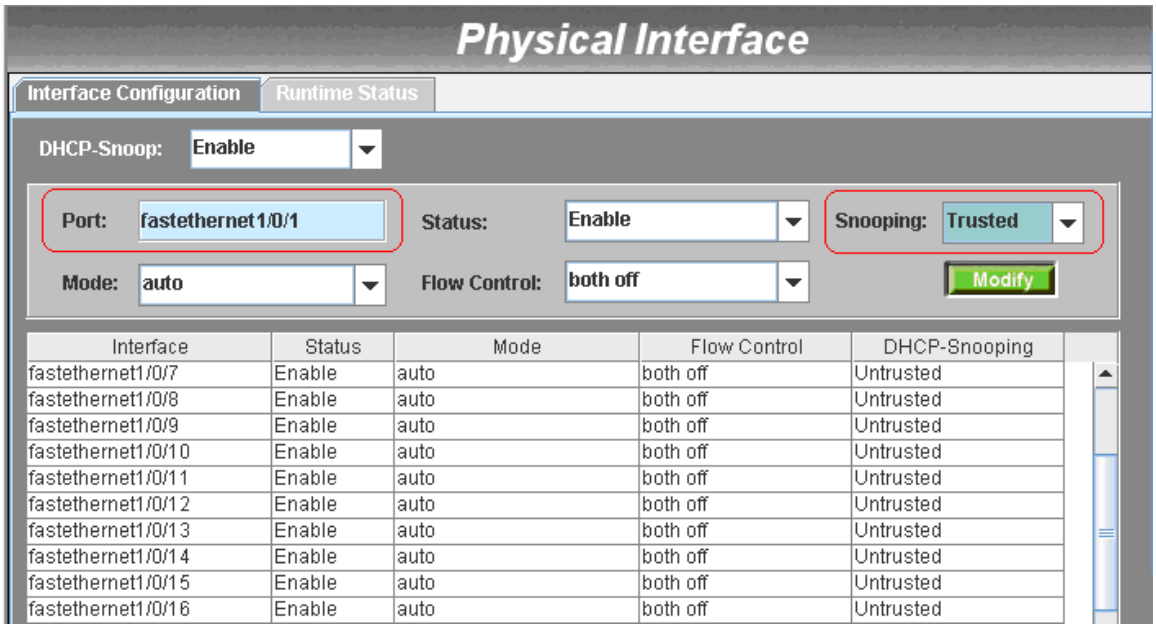


After enable this function globally, go to VLAN configuration page, type in the VLAN id you want to configure, and select 'Enable' at 'DHCP-Snooping' item, then click 'summit' to apply the configuration setting.



The final step is setting which physical interface that your DHCP server connected. By default, all interfaces are untrusted.

Select 'Trusted' at 'Snooping' item after you choice a interface, then click "Summit' to finish your configuration of all.



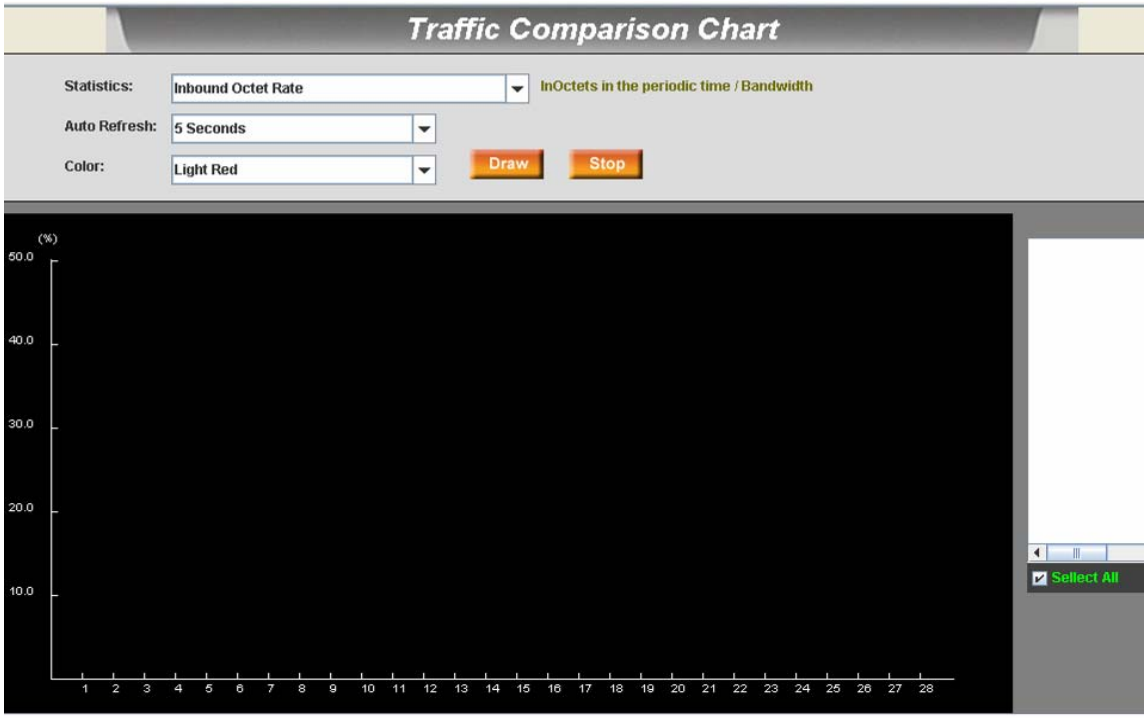
7.11 Traffic Chart

These statistical chart pages provide network flow information. The user can specify the time limits for chart refresh updates. The charts allow the user to monitor different types of network traffic. Most MIB-II counters are displayed in these charts.

Auto Refresh sets the time interval at which new data is retrieved from the switch. **Color** lets the user assign a different color to each variable. After the variables have been set, **Draw** lets the browser draw the graphic chart. Each new Drawing will reset the statistics display.

7.11.1 Traffic Comparison Chart

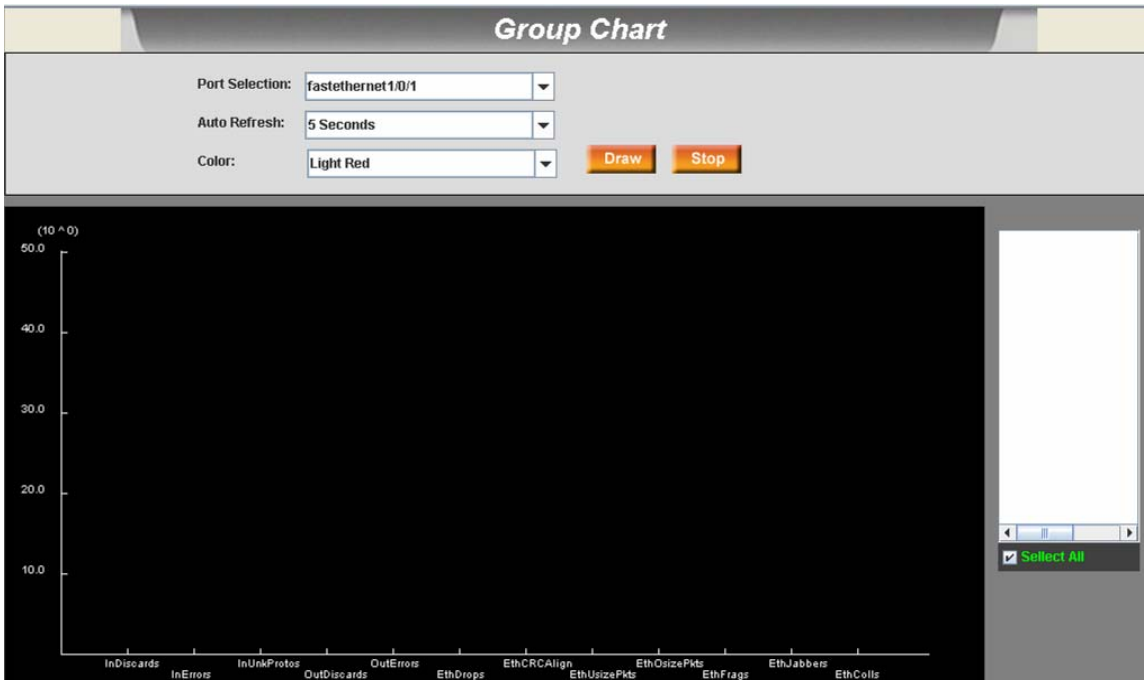
This page shows one statistic for all the ports in one graphic chart. Specify the statistic to be displayed and then click **Draw**. The browser will refresh the graph periodically.



Traffic Comparison Chart

7.11.2 Group Chart

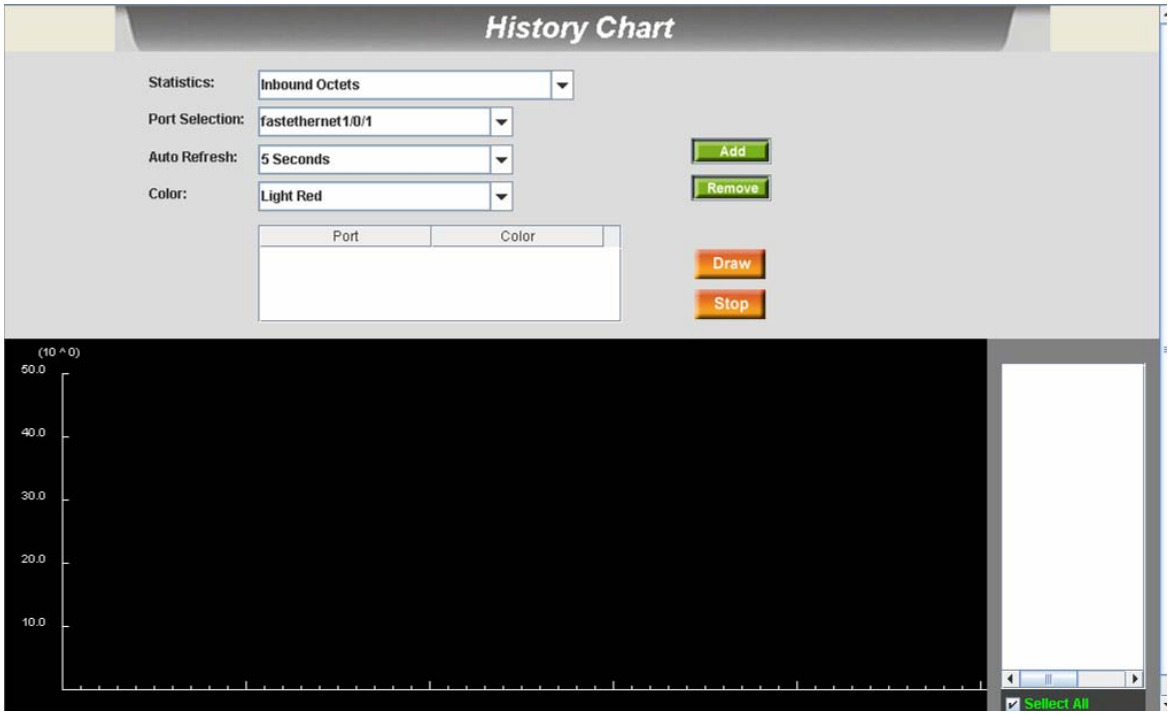
Select the Port, Refresh Period and display Color, then click **Draw**. The statistics window shows all the discards or error counts for the specified port. Data is updated periodically.



Group Chart

7.11.3 History Chart

The user can display information for different ports and statistics items in this chart. Since this shows the history of the statistics information, the line chart keeps the old data even when it is refreshed.



History Chart

7.12 Save Configuration

Click **Save** to make the settings permanent by saving to the Flash memory (**Submit** only saves changes to the RAM memory and such changes will be lost if the Switch is switched off).

To reset the Switch's configuration, click on **OK** to reset the configuration file to factory default. A system reboot will follow this restoration process.

> **NOTE:** All user configurations will be lost when you choose to restore the factory default configuration.

Save Configuration

8 Command Line Interface

This chapter describes how to use console interface to configure the switch. The switch provides RS232 connectors to connect to a PC. Use a terminal emulator on the PC, such as HyperTerminal or command line interpreter, to configure the switch. The terminal emulator should be configured with a baud rate of 38400, 8 bit data, no parity, 1 stop bit, and no flow control.
In CLI mode, typing "?" will display all available command help messages. All the CLI commands are case sensitive.

8.1 Power On

Power On Self Test is executed during the system booting period. It tests system memory, LED and hardware chips on the switchboard. It displays system information as the result of system testing and initialization. The user can ignore all information until the prompt, "Switch login:" appears.

8.1.1 Boot ROM command mode

During the POST process, you can enter a "Boot ROM Command" mode by pressing the <**ENTER**> key. Type the "?" key to show the help messages for all available commands.

> **Note:** *Although the commands are helpful in some situations, we **STRONGLY** advise users not to use them if they do not know the command function.*

8.1.2 Boot ROM Commands

The following are two types of boot ROM commands,

- "command": The current settings will be displayed.
- "command" with new setting: The current setting will be replaced by a specified new setting.

Command	Parameters	Usage	Notes
Baud rate	Baud Rate	9600 38400 57600 115200	The user should set up the terminal emulator with the same baud rate to make it work
bdinfo	none	none	print Board Info structure
echo	string	none	echo the string to console
ethaddr	none	none	get MAC address
gatewayip	IP address	xxx.xxx.xxx.xxx	set gateway IP address
go	none	none	boot firmware image
? or help	none	none	print online help
imls	none	none	list all images found in flash
ipaddr	IP address	xxx.xxx.xxx.xxx	set tftp client IP address

loadbx	none	none	load binary file over serial line (X modem)
netmask	mask	xxx.xxx.xxx.xxx	set network mask
ping	host	xxx.xxx.xxx.xxx	send ICMP ECHO_REQUEST to network host
pwd	none	none	reset switch password
reset	none	none	perform reset of the CPU
serverip	IP address	xxx.xxx.xxx.xxx	set tftp server IP address
slot	slot	1, 2, auto	select boot slot to boot
tftpboot	filename	Example: 3112single.img	load image via network using TFTP protocol
version	none	none	print monitor version

Boot ROM commands

8.2 Login and Logout

To enter the CLI mode, a valid user name and password must be entered. For the first login, the user can enter “admin” as the user name (without password). For security reasons, please change the user name and password after login. If you forget the user name and password, you may contact the support team or restore the default user account in the Boot ROM Command mode – “pwd”. If you select the second choice, the default username “admin” will be restored.

Type “exit” to leave the CLI mode safely. This action allows the user to secure the CLI mode. The next user has to log in again with an authorized user name and password.

8.3 CLI Commands

The Switch provides CLI commands for all managed functions. The user can follow the instructions and set up the switch correctly as easily as using WEB interface to configure the switch.

Note: *Always use “?” or “list” to get the available commands list and help.*

Always use “end” to get back to the root directory (enable mode).

8.3.1 User Account

8.3.1.1 Add user

Add a new user or modify an existing user’s password.

CLI Syntax: add user user-name password

Example: `Switch(config)#add user admin 123`

8.3.1.2 Delete user

Delete an existing user.

CLI Syntax: delete user user-name

Example: `Switch(config)#delete user admin`

8.3.2 Backup and Restore

8.3.2.1 Backup start-up configuration file

Backup the start-up configuration file “Quagga.conf” of the switch to TFTP server.

CLI Syntax: copy startup-config tftp: URL

Example: `Switch#copy startup-config tftp: 192.168.8.56`

8.3.2.2 Restore start-up configuration file

Restore the start-up configuration file “Quagga.conf” of the switch from TFTP server.

CLI Syntax: copy tftp: URL startup-config

Example: `Switch#copy tftp: 192.168.1.2 startup-config`

8.3.3 System Management Configuration

8.3.3.1 Firmware Upgrade

Upgrade new firmware into the Switch.

CLI Syntax: archive download-sw /overwrite tftp_server ImageFile

Example: **Switch(config)#archive download-sw / overwrite 192.1.1.1 3112single.img**

> **Notes:** *We strongly recommend that you back up “startup-config” before upgrading.*

8.3.3.2 Configure Terminal

Use the write configuration command on the switch to configure.

CLI Syntax: configure terminal

Example: `Switch#configure terminal`

8.3.3.3 Enable

Enter enable mode and turn on privileged mode command.

CLI Syntax: enable

Example: `Switch>enable`

8.3.3.4 Disable

Exit enable mode and turn off privileged mode command.

CLI Syntax: disable

Example: `Switch#disable`

8.3.3.5 End

This command lets the user end the current mode and go to enable mode.

CLI Syntax: end

Example: `Switch(config)#end`

8.3.3.6 Exit

This command lets the user end the current mode and go to the previous mode.

CLI Syntax: exit

Example: `Switch#exit`

8.3.3.7 Help

This command lists all the commands of the operational mode.

CLI Syntax: list

Example: `Switch#list`

Example: `Switch#?`

8.3.3.8 Host name

Displays the given name of the switch. This is an RFC-1213-defined MIB object in System Group, and provides administrative information on the managed node.

CLI Syntax: hostname WORD

Example: `Switch(config)#hostname Switch`

If the user enters a name in the name description field, the Switch's system name changes to the new one.

8.3.3.9 Date

Set system date/time.

CLI Syntax: date STRING(MMDDhhmmYYYY)

Example: `Switch#date 080112202007`

8.3.3.10 System Contact

Displays contact information regarding the Switch. This is an RFC-1213-defined MIB object in System Group, and provides contact information on the managed node.

CLI Syntax: snmp-server contact WORD

Example: `Switch(config)#snmp-server contact clerk@central.com.tw`

If the user puts the contact info in the contact description field, the Switch's contact info will change to the new info.

8.3.3.11 System Location

Displays the physical location of the switch. This is an RFC-1213-defined MIB object in System Group, and provides the location information on the managed node.

CLI Syntax: snmp-server location WORD

Example: `Switch(config)#snmp-server location Central-Building`

Type in the new location description in the location description field.

8.3.3.12 IP Address and Network Mask

Displays the Switch's IP address. This IP address is used for managing purposes, i.e.; network applications such as, the http server, SNMP server, tftp server, ssh and telnet server of the Switch are all using this IP address in interface vlan1.

CLI Syntax: ip address A.B.C.D/M

Example: `Switch(config)#interface vlan 1`

```
Switch(config-if)#ip address 192.168.20.121/24
```

8.3.3.13 Reboot

Use this command to reboot the system.

CLI Syntax: reboot

Example: `Switch(config)#reboot`

8.3.3.14 Reload

Use this command to copy a default-config file to replace the current one.

CLI Syntax: reload default-config file

Example: `Switch#reload default-config file`

8.3.3.15 show running-config

To show running-config file.

CLI Syntax: show running-config

Example: `Switch#show running-config`

8.3.3.16 write memory

Use the write file configuration command on the switch stack or standalone switch to write configuration to the file.

CLI Syntax: write memory

Example: `Switch#write memory`

8.3.3.17 Assign a new user account

Add a user, e.g. a user named tony whose password is tony123456

CLI Syntax: add user WORD WORD

Example: `Switch(config)#add user tony tony123456`

8.3.3.18 Delete a new user account

Delete a user account, e.g. for a user named tony.

CLI Syntax: delete user WORD

Example: `Switch(config)#delete user tony`

8.3.4 Physical interface commands

8.3.4.1 Interface mode

Use the auto-negotiation configuration command on the switch to set the auto-negotiation status of the port.

CLI Syntax: auto-negotiation

Example:
```
Switch(config)#interface fastethernet1/0/2
Switch(config-if)#auto-negotiation
```

This example shows how to use the auto-negotiation configuration command on the switch to enable auto-negotiation mode.

8.3.4.2 Interface duplex

Use the duplex configuration command on the switch to set duplex status of the port.

CLI Syntax: duplex (full| half)

Example: **Switch(config)#interface fastethernet1/0/2**

Switch(config-if)#duplex full

This example shows how to use the duplex configuration command on the switch to set full-duplex on the interface.

8.3.4.3 Interface flow control

Use the flow control configuration command on the switch to set flow control status of the port.

CLI Syntax: flowcontrol (rx| tx | both) (on|off)

Example: **Switch(config)#interface fastethernet1/0/2**

Switch(config-if)#flowcontrol both on

This example shows how to use the flow control configuration command on the switch to set 'flow control both on'.

8.3.4.4 Show L2 interface

Use the show l2_interface command on the switch to show l2 interface status.

CLI Syntax: show l2_interfaces IFNAME

Example: **Switch#show l2_interface fastethernet1/0/2**

8.3.5 IP interface

8.3.5.1 Show vlan name string

Use the show vlan user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the Switch.

CLI Syntax: show vlan name string

Example: **Switch#show vlan name VLAN1**

Note: VLAN1 is for system purposes like firmware upgrade, management, etc.

8.3.5.2 Create a vlan entry

Use the vlan id command to create a vlan entry on the Switch. Use the name string command to create a vlan entry with a string on the Switch.

CLI Syntax: vlan id

Example: **Switch(config)#vlan 3**

Switch(config-vlan)#name vlan3

8.3.5.3 Interface vlan VLAN-ID

This command changes the operation to vlan interface command mode.

CLI Syntax: interface vlan VLAN-ID

Example: **Switch(config)#interface vlan 1**

8.3.5.4 IP address

This command sets the ip address for a specific interface.

CLI Syntax: ip address A.B.C.D/M

Example: **Switch(config)#ip address 192.168.20.121/24**

Note: This will not show the interface name. Please remember which interface you are configuring.

8.3.5.5 IP helper-address

This command enables DHCP relay for a specific interface

CLI Syntax: ip helper-address A.B.C.D

Example: **Switch(config-if)#ip helper-address 192.168.1.180**

8.3.5.6 IP OSPF

This command sets up OSPF interface parameters

CLI Syntax: ip ospf

Example: **Switch(config-if)#ip ospf cost 100**

8.3.5.7 IP PIM

This command sets up PIM-DM interface parameters

CLI Syntax: ip pim

Example: **Switch(config-if)#ip pim dense-mode**

8.3.5.8 IP RIP

This command sets up RIP interface parameters

CLI Syntax: ip rip

Example: **Switch(config-if)#ip rip send version 1**

8.3.6 RIP

8.3.6.1 Router RIP

The router rip command is necessary to enable RIP. To disable RIP, use the ‘no router rip’ command. RIP must be enabled before carrying out any of the RIP commands.

CLI Syntax: router rip

Example: **`Switch(config)#router rip`**

8.3.6.2 No Router RIP

Disable RIP.

CLI Syntax: no router rip

Example: **`Switch(config)#no router rip`**

8.3.6.3 Version

RIP can be configured to process either Version 1 or Version 2 packets. The default mode is Version 2.

CLI Syntax: version 1|2

Example: **`Switch(config-router)#version 1`**

8.3.6.4 Network

Set the RIP-enable interfaces via network. Interfaces with addresses matching the network’s are enabled.

CLI Syntax: network A.B.C.D/M

Example: **`Switch(config-router)#network 35.0.0.0/8`**

8.3.7 OSPF

8.3.7.1 Router OSPF

Enable or disable the OSPF process. OSPFD does not support multiple OSPF processes, so the user cannot specify an OSPF process number.

CLI Syntax: router ospf

Example: **`Switch(config)#router ospf`**

8.3.7.2 Router ID

Assign an OSPF Router ID in IP-address format.

CLI Syntax: ospf router-id a.b.c.d

Example: **`Switch(config-router)#ospf router-id 10.0.0.3`**

8.3.7.3 Area

Set the OSPF area ID.

CLI Syntax: network a.b.c.d/m area decimal-value

Example: **`Switch(config-router)#network 102.192.2/24 area 1`**

8.3.8 VRRP

Enable or disable VRRP functions for a specific IP interface.

CLI Syntax: standby VRID (1-255) ip a.b.c.d

Example: **`Switch(config-if)#standby 1 ip 192.168.1.1`**

8.3.9 Spanning Tree

8.3.9.1 clear spanning-tree counters

Use the ‘clear spanning-tree counters’ configuration command on the switch to clear spanning-tree statistics.

CLI Syntax: clear spanning-tree counters

Example: **`Switch#clear spanning-tree counters`**

8.3.9.2 clear spanning-tree counters interface IFNAME

Use the ‘clear spanning-tree counters’ configuration command on the switch to clear spanning-tree statistics on one interface.

CLI Syntax: clear spanning-tree counters interface IFNAME

Example: **`Switch#clear spanning-tree counters interface fastethernet1/0/2`**

8.3.9.3 default spanning-tree

This command sets spanning-tree parameter to default.

CLI Syntax: default spanning-tree

Example: **`Switch#default spanning-tree forward-time`**

8.3.9.4 show spanning-tree active

To ‘show spanning-tree active’.

CLI Syntax: show spanning-tree active

Example: `Switch#show spanning-tree active`

8.3.9.5 spanning-tree enable and disable

Enable/Disable the spanning tree.

CLI Syntax: spanning-tree (enable|disable)

Example: `Switch#spanning-tree disable`

8.3.10 Link Aggregation

8.3.10.1 trunk aggregation group

Use the aggregation-link trunk group configuration command on the switch to configure trunk aggregation group.

CLI Syntax: aggregation-link trunk STACKID group <1-32> PORTLIST

Example: `Switch#aggregation-link trunk 1 group 1 25,26`

8.3.10.2 trunk load balancing

Use the aggregation-link trunk group configuration command on the switch to configure trunk load balancing by using source-based or destination-based forwarding methods.

CLI Syntax: aggregation-link trunk STACKID load-balance group <1-32> (src-mac |dst-mac |src-dst-mac |src-ip |dst-ip |src-dst-ip)

Example: `Switch#aggregation-link trunk 1 load-balance group 1`

8.3.10.3 show aggregation-link trunk

To ‘show aggregation-link trunk’ status.

CLI Syntax: show aggregation-link trunk STACKID [GROUPID]

Example: `Switch#show aggregation-link trunk 1 1`

8.3.11 LACP

8.3.11.1 clear lacp counters

Use the ‘clear lacp counters’ configuration command on the switch to clear the statistics for all aggregated port sets.

CLI Syntax: clear lacp counters [STACKID]

Example: **`Switch#clear lacp counters 1`**

8.3.11.2 lacp aggregation-link trunk

This command sets the Link Aggregation Control Protocol (LACP) operation add/set for the trunk group ports on the switch.

CLI Syntax: lacp aggregation-link trunk STACKID (add/set) group <1-32> PORTLIST

Example: **`Switch#lacp aggregation-link trunk 1 set group 1 25,26`**

8.3.11.3 disable lacp aggregation-link trunk

This command sets the Link Aggregation Control Protocol (LACP) operation add/set or disable for the trunk group ports on the switch.

CLI Syntax: lacp aggregation-link trunk STACKID disable port-number

Example: **`Switch#lacp aggregation-link trunk 1 disable 26`**

8.3.11.4 lacp port-priority

This command sets the port priority for the Link Aggregation Control Protocol (LACP) on the switch.

CLI Syntax: lacp port-priority <1-65535>

Example: **`Switch(config)#interface giga1/0/26`**

`Switch(config-if)#lacp port-priority 1000`

8.3.11.5 lacp system-priority

This command sets the system priority for the Link Aggregation Control Protocol (LACP) on the switch.

CLI Syntax: lacp system-priority <1-65535>

Example: **`Switch(config)#lacp system-priority 20000`**

8.3.12 Mirroring

8.3.12.1 mirror mode

To set port mirror mode (layer 2).

CLI Syntax: mirror mode

Example: **`Switch(config)# mirror mode enable`**

8.3.12.2 mirror setting

This command mirrors the source interface list traffic to the destination interface. The mirror type supports Received traffic, Transmitted traffic, or both.

CLI Syntax: mirror IFLIST to IFNAME (rx|tx|both)

Example: `Switch(config)#mirror fastethernet1/0/3-5 to fastethernet1/0/9 both`

8.3.12.3 show mirror

To show current mirror features.

CLI Syntax: Show mirror

Example: `Switch#show mirror`

8.3.12.4 no mirror

This command resets the source interface's received or transmitted traffic or both the destination interface.

CLI Syntax: no mirror SRCIFLIST (rx|tx|both)

Example: `Switch(config)#no mirror fastethernet1/0/2 rx`

8.3.13 Static Multicast

8.3.13.1 mac-address-table multicast

Use the mac-address-table multicast configuration command on the switch to add multicast static addresses to the MAC address table.

CLI Syntax: mac-address-table multicast MACADDR vlan VLANID interface IFLIST

Example: `Switch(config)#mac-address-table multicast 0100.5e11.1111 vlan 2 interface fastethernet1/0/3 1`

8.3.13.2 no mac-address-table multicast

Use the no mac-address-table multicast configuration command on the switch to remove multicast static port from the MAC address table.

CLI Syntax: no mac-address-table multicast MACADDR vlan VLANID interface IFLIST

Example: `Switch(config)#no mac-address-table multicast 0100.5e11.1111 vlan 2 interface fastethernet1/0/3 1`

8.3.13.3 show mac-address-table multicast

Use the 'show mac-address-table multicast' user EXEC command to display the Layer 2 multicast entries for all VLANs. Use the command in privileged EXEC mode to display specific multicast entries.

CLI Syntax: show mac-address-table multicast

Example: `Switch#show mac-address-table multicast`

8.3.14 IGMP Snooping

8.3.14.1 disable ip igmp snooping

This command disables the 'ip igmp snooping' feature.

CLI Syntax: no ip igmp snooping

Example: `Switch(config)#no ip igmp snooping vlan 1`

8.3.14.2 ip igmp snooping

This command sets the IGMP snooping function to enabled globally.

CLI Syntax: ip igmp snooping

Example: `Switch(config)#ip igmp snooping vlan 1`

8.3.14.3 interval time

This command sets the interval time for the IGMP queries sent by the Switch.

CLI Syntax: ip igmp snooping last-member-query-interval TIMEVALUE

Example: `Switch(config)#ip igmp snooping last-member-query-interval 100`

8.3.15 Traffic Control

8.3.15.1 storm-control

Use the storm-control configuration command on the Switch to set the limit rate of the port's total bandwidth used by broadcast/dlf/multicast.

CLI Syntax: storm-control (broadcast|dlf|multicast) LIMIT_RATE

Example: `Switch(config-if)#storm-control broadcast 25`

8.3.15.2 no storm-control

Use the no storm-control configuration command on the switch to disable the limit rate of the port's total bandwidth used by broadcast/dlf/multicast.

CLI Syntax: no storm-control (broadcast|dlf|multicast)

Example: `Switch(config-if)#no storm-control broadcast`

8.3.15.3 show storm-control

Use the show storm-control configuration command on the switch to show the limit rate of the port's total bandwidth used by broadcast/dlf/multicast.

CLI Syntax: show storm-control IFNAME (broadcast|dlf|multicast)

Example: `Switch#show storm-control gi1/0/1 broadcast`

8.3.16 Dynamic Addresses

8.3.16.1 clear dynamic mac-address

Use the write configuration command on the switch stack or standalone Switch to clear dynamic L2 MAC addresses in the database.

CLI Syntax: clear mac-address-table dynamic address MAC_ADDR

Example: `Switch(config)#clear mac-address-table dynamic address 0000.1111.2222`

8.3.16.2 aging time

Use the mac-address-table aging-time configuration command on the switch stack or on a standalone Switch to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.

The real aging time is triple the command input radix number (in seconds).

CLI Syntax: mac-address-table aging-time <1-255>

Example: `Switch(config)#mac-address-table aging-time 100`

This example shows how to configure the mac-address-table aging time to 300 seconds.

8.3.16.3 no aging time

Disables the aging timer of the mac-address-table.

CLI Syntax: no mac-address-table aging-time

Example: `Switch(config)#no mac-address-table aging-time`

8.3.16.4 show mac-address-table aging-time

CLI Syntax: show mac-address-table aging-time

Example: `Switch#show mac-address-table aging-time`

8.3.17 Static Addresses

8.3.17.1 add static mac-address

The user can add a MAC address to the Switch address table. The MAC address added this way will not age out from the address table. This is called a static address.

CLI Syntax: mac-address-table static MAC_ADDR vlan VLANID interface IFNAME

Example: `Switch(config)#mac-address-table static 0000.1111.2222 1 fastethernet1/0/2`

8.3.17.2 show mac-address-table

This shows static and dynamic mac-addresses.

CLI Syntax: show mac-address-table

Example: `Switch#show mac-address-table`

8.3.18 VLAN

8.3.18.1 show vlan name string

Use the ‘show vlan’ user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

CLI Syntax: show vlan name string

Example: `Switch#show vlan name VLAN1`

8.3.18.2 vlan vid

Use the vlan vid command to create a vlan entry on the switch.

CLI Syntax: vlan vid

Example: `Switch(config)#vlan 2`

8.3.18.3 name string

Use the ‘name string’ command to create a vlan entry with a string on the switch.

CLI Syntax: name string

Example: `Switch(config-vlan)#name VLAN2`

8.3.18.4 access vlan

Set access mode characteristics of all interfaces and Set Virtual LAN.

CLI Syntax: switchport access vlan <1-4094>

Example: **Switch(config)# interface fastethernet1/0/2**
Switch(config-if)#switchport access vlan 1

8.3.18.5 allowed VLANs

Use the 'switchport trunk allowed vlan' configuration command on the Switch to add or remove the VLANs that are allowed to receive and send traffic on this interface in tagged format when in trunking mode

CLI Syntax: switchport trunk allowed vlan (add|remove) VLANLIST

Example: **Switch(config)# interface fastethernet1/0/2**
Switch(config-if)#switchport trunk allowed vlan add 1

8.3.19 GVRP

8.3.19.1 clear gvrp statistics

Use the 'clear gvrp statistics' configuration command on the switch to clear all the GVRP statistics information on one or all interfaces.

CLI Syntax: clear gvrp statistics [IFNAME]

Example: **Switch#clear gvrp statistics fastethernet1/0/2**

8.3.19.2 default gvrp configuration

This command sets the GVRP configuration to default.

CLI Syntax: default gvrp configuration

Example: **Switch#default gvrp configuration**

8.3.19.3 gvrp mode

This command sets the GVRP feature to globally be enabled or disabled on the switch.

CLI Syntax: gvrp mode (enable|disable)

Example: **Switch#gvrp mode enable**

8.3.19.4 show gvrp configuration

To show gvrp configuration IFNAME status.

CLI Syntax: show gvrp configuration IFNAME

Example: **Switch#show gvrp configuration fastethernet1/0/1**

8.3.19.5 show gvrp portstate

To show gvrp statistics IFNAME status.

CLI Syntax: show gvrp portstate [IFNAME] VID

Example: `Switch#show gvrp portstate fastethernet1/0/1 1`

8.3.20 CoS/QoS

8.3.20.1 queue cos-map

Use the ‘queue cos-map configuration’ command on the switch to select the CoS queue that a given priority should map into.

CLI Syntax: queue cos-map PRIORITY QUEUE

Example: `Switch(config)#queue cos-map 1 3`

8.3.20.2 show queue cos-map

This command shows the information of CoS and priority mapping.

CLI Syntax: show queue cos-map

Example: `Switch#show queue cos-map`

8.3.20.3 qos mode

This command sets qos mode to high_first mode.

CLI Syntax: qos mode high_first

Example: `Switch(config)#qos mode high_first`

8.3.20.4 show qos mode

This command shows the qos mode.

CLI Syntax: show qos mode

Example: `Switch#show qos mode`

8.3.20.5 qos egress bandwidth

This command is used to set the QoS bandwidth informational parameter for the outgoing packets.

CLI Syntax: qos egress bandwidth LIMIT_RATE

Example:
```
Switch(config)# interface fastethernet1/0/2
        Switch(config-if)#qos egress bandwidth 100
```

8.3.21 SNMP

8.3.21.1 show rmon statistics

To show rmon statistics IFNAME status.

CLI Syntax: show rmon statistics [IFNAME]

Example: `Switch#show rmon statistics fastethernet1/0/1`

8.3.21.2 show snmp-server community

To show snmp-server community.

CLI Syntax: show snmp-server community

Example: `Switch#show snmp-server community`

8.3.21.3 snmp-server host

This command sets the SNMP host information.

CLI Syntax: snmp-server host A.B.C.D

Example: `Switch(config)#snmp-server host 192.168.8.31`

8.3.22 Filter

8.3.22.1 deny any host

Use this deny MAC access list configuration command on the switch to prevent non-IP traffic from being forwarded if the conditions are matched. Use the no form of this command to remove a deny condition from the named MAC access list.

CLI Syntax: deny any host MACADDR [VLANID]

Example:
```
Switch(config)# mac access-list extended mac_acl
        Switch(config-ext-macl)#deny any host c2f3.220a.12f4 1
```

8.3.22.2 filter set

This command defines an extended MAC access list using a name, and enter access-list configuration mode.

CLI Syntax: mac access-list extended WORD

Example: `Switch(config)#mac access-list extended mac_acl_1`

8.3.22.3 filter conditions

This command specifies one or more conditions (denied or permitted) to decide if the packet is forwarded or dropped.

CLI Syntax: (permit|deny) any any IFNAME

Example: `Switch(config-ext-macl)#permit any any 1`

8.3.22.4 filter attach

This command is used to assign filter rule for a specific port.

CLI Syntax: mac access-group WORD in

Example: `Switch(config-if)#mac access-group mac_acl_1 in`

8.3.23 Port Access Control

8.3.23.1 default system authentication control

This command sets dot1x system authentication control to default.

CLI Syntax: default dot1x system-auth-control

Example: `Switch(config)#default dot1x system-auth-control`

8.3.23.2 dot1x default

This command resets the configurable 802.1x parameters to the default values.

CLI Syntax: dot1x default

Example:
```
Switch(config)#interface fastethernet1/0/1
Switch(config-if)# dot1x default
```

8.3.23.3 dot1x guest-vlan

Use the dot1x guest-vlan interface configuration command on the switch to specify an active VLAN as an 802.1X guest VLAN. Use the no form of this command to return to the default setting.

CLI Syntax: dot1x guest-vlan <1-255>

Example:
```
Switch(config)#interface fastethernet1/0/1
Switch(config-if)# dot1x guest-vlan 3
```

8.3.23.4 dot1x initialize interface

Use the ‘dot1x initialize privileged’ EXEC command on the switch to manually return the specified 802.1X-enabled interface to an unauthorized state before initiating a new authentication session on the interface.

CLI Syntax: dot1x initialize interface [IFNAME]

Example:
```
Switch#dot1x initialize interface fastethernet1/0/1
```

8.3.23.5 dot1x max-req

Use the dot1x max-req interface configuration command on the switch to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the no form of this command to return to the default setting.

CLI Syntax: dot1x max-req <1-10>

Example:
```
Switch(config)#interface fastethernet1/0/1
Switcjh(config-if)#dot1x max-req 2
```

8.3.23.6 dot1x port-control

Use the dot1x port-control interface configuration command on the switch to enable manual control of the authorization state of the port. Use the no form of this command to return to the default setting.

CLI Syntax: dot1x port-control (auto|force-authorized| force-unauthorized)

Example:
```
Switch(config)#interface fastethernet1/0/1
Switch(config-if)#dot1x port-control force-authorized
```

8.3.24 Dial-in User

8.3.24.1 dot1x username password

Add user into local radius database.

CLI Syntax: dot1x username WORD passwd WORD vlan

Example: `Switch(config)#dot1x username test passwd 12345 vlan 1`

8.3.24.2 show dot1x user

Show dot1x dial-in user.

CLI Syntax: show dot1x username

Example: `Switch#show dot1x username`

8.3.25 RADIUS

8.3.25.1 RADIUS settings

This command sets the radius server ip, radius key, and radius port for 802.1X configuration.

CLI Syntax: dot1x radius server-ip A.B.C.D key RADIUS_KEY [PORTID]

Example: `Switch(config)#dot1x radius server-ip 192.168.1.38 key 123456 1812`

8.3.25.2 show dot1x radius

Show dot1x radius server ip, radius key, and radius port for 802.1X configuration.

CLI Syntax: show dot1x radius

Example: `Switch#show dot1x radius`

8.4 Miscellaneous commands

show modelname: shows the model name of switch.

show version: shows the hardware, boot rom and firmware version.

ping: ping remote host

show vlan_all: display vlan

show ip route: display the entries in the routing table

9 Contact Information

VOLKTEK CORPORATION

4F, No. 192 Lian-Cheng Road
Chung-Ho, Taipei 235, Taiwan ROC

TEL: +886-2-8242-1000
FAX: +886-2-8242-3333
Tech Support: +886-800-286-286

ISO 9001 Certified